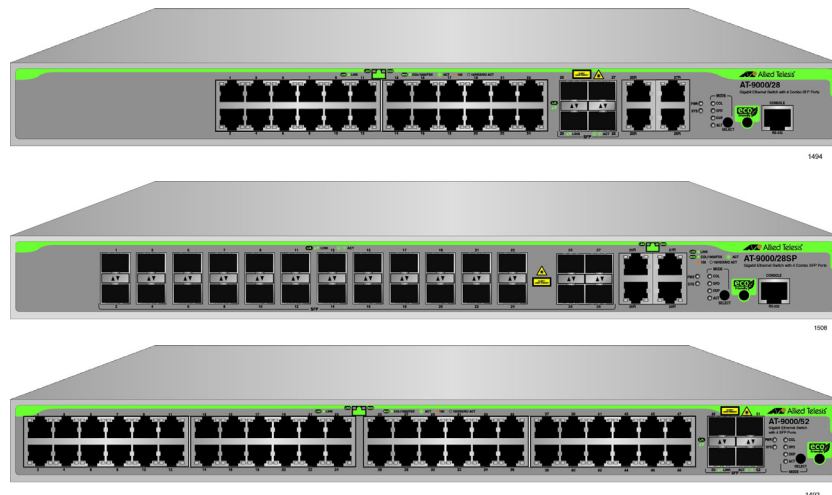Allied Telesis™

AT-9000 Series

Gigabit Ethernet Switches

- ❏ AT-9000/12PoE
- ❏ AT-9000/28
- ❏ AT-9000/28PoE
- ❏ AT-9000/28SP
- ❏ AT-9000/52

Management Software Command Line Interface User's Guide

AlliedWare Plus Version 2.1.8.0

613-001823 Rev. B

Copyright

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 this product, 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, Inc.
3041 Orchard Parkway
San Jose, California 95134

No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, AlliedWare Plus, and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

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

Contents

5

Contents

Contents

12

18

20

Contents

28

Figures

32

Tables

Tables

36

Preface

This is the command line management guide for the AT-9000/12POE, AT-9000/28, AT-9000/28POE, AT-9000/28SP, and AT-9000/52 Managed Layer 2-4 Gigabit Ethernet EcoSwitches. The instructions in this guide explain how to start a management session and how to use the commands in the AlliedWare Plus command line interface to view and configure the features of the switch.

For hardware installation instructions, refer to the AT-9000 *Manager Layer 2 Fast Ethernet EcoSwitch Series Installation Guide*.

This preface contains the following sections:

❒ "Document Conventions" on page 38

❒ "Where to Find Web-based Guides" on page 39

❒ "Contacting Allied Telesis" on page 40

> ⚠ **Caution**
>
> The customer, re-seller, sub-contractor, distributor, software developer or any buyer of an Allied Telesis "ATI" product known as "customer", hereby agrees to have all licenses required by any governmental agency and to comply with all applicable laws and regulations in its performance under this Agreement, including export control, maintained by U.S. Commerce Department's Bureau of Industry and Security (BIS) and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), international boycotts regulations and all anti-corruption laws, including the U.S. Foreign Corrupt Practices Act (FCPA). The customer understands that U.S. Government authorization may be required to export the software, commodity or technology, or to re-export or re-transfer to a third country, another end-user or another end-use. The customer agrees to assume all such obligations.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

38

Where to Find Web-based Guides

The installation and user guides for all of the Allied Telesis products are available for viewing in portable document format (PDF) from our web site at **www.alliedtelesis.com/support/documentation**.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

❒ 24/7 Online Support— Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis experts.

❒ USA and EMEA phone support— Select the phone number that best fits your location and customer type.

❒ Hardware warranty information— Learn about Allied Telesis warranties and register your product online.

❒ Replacement Services— Submit a Return Materials Authorization (RMA) request via our interactive support center.

❒ Documentation— View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.

❒ Software Downloads— Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase** and select your region.

Section I
Getting Started

This section contains the following chapters:

42

Chapter 1

AlliedWare Plus Command Line Interface

This chapter has the following sections:

Management Sessions

You can manage the switch locally or remotely. Local management is conducted through the Console port on the switch. Remote management is possible with a variety of management tools from workstations on your network.

Local Management

The switch has a Console port for local management of the unit. Local management sessions, which must be performed at the unit, hence the name "local," are commonly referred to as out-of-band management because they are not conducted over your network.

The requirements for local management sessions are a terminal or a PC with a terminal emulator program and the RS-232 console management cable that comes with the switch. For modern PCs without a serial port, a USB-to-serial adapter and driver software is required.

> **Note**
> The initial management session of the switch must be from a local management session.

Remote Management

You can manage the switch remotely with the following software tools:

❏ Telnet client

❏ Secure Shell client

❏ Secure (HTTPS) or non-secure (HTTP) web browser

❏ SNMPv1, SNMPv2c, or SNMPv3 application

Management sessions performed with these tools are referred to as in-band management because the sessions are conducted over your network. Remote management sessions are generally more convenient than local management session because they can be performed from any workstation that has one of these software tools.

Table 1. Remote Software Tool Settings

Software Tool	Default Setting
Telnet	Enabled
Secure Shell Server	Disabled
HTTPS	Disabled
HTTP	Enabled (This tool is disabled by a factory reset of the switch.)

To support remote management, the switch must have a management IP address. For instructions on how to assign a management IP address to the switch, refer to "Adding a Management IP Address" on page 72.

Remote Telnet Management

The switch has a Telnet server that you can use to remotely manage the unit from Telnet clients on your management workstations. Remote Telnet sessions give you access to the same commands and the same management functions as local management sessions.

> **Note**
> Telnet remote management sessions are conducted in clear text, leaving them vulnerable to snooping. If an intruder captures the packet with your login name and password, the security of the switch will be compromised. For secure remote management, Allied Telesis recommends Secure Shell (SSH) or secure web browser (HTTPS).

Remote Secure Shell Management

The switch has an SSH server for remote management with an SSH client on a management workstation. This management method is similar to Telnet management sessions in that it gives you access to the same command line interface and the same functions. But where they differ is SSH management sessions are secure against snooping because the packets are encrypted, rendering them unintelligible to intruders who might capture them.

For instructions on how to configure the switch for SSH management, refer to Chapter 82, "Secure Shell (SSH) Server" on page 1329.

Web Browser Windows

The switch comes with a web browser server so that you can manage the unit using a web browser on a management workstation. The switch supports both encrypted (HTTPS) and non-encrypted (HTTP) web browser management sessions.

Simple Network Management Protocol

The switch supports remote SNMPv1, SNMPv2c and SNMPv3 management. This form of management requires an SNMP application, such as AT-View, and an understanding of management information base (MIB) objects.

The switch supports the following MIBs for SNMP management:

- atistackinfo.mib
- atiEdgeSwtich.mib
- RFC 1155 MIB
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1643 Ethernet MIB
- RFC 2096 IP Forwarding Table MIB
- RFC 2790 Host MIB
- RFC 2863 Interface Group MIB
- RFC 3176 sFlow MIB
- IEEE 802.1x 2010 MIB

The Allied Telesis managed switch MIBs (atistackinfo.mib and atiEdgeSwitch.mib) are available from the Allied Telesis web site.

Management Interfaces

The switch has two management interfaces:

❒ AlliedWare Plus command line

❒ Web browser windows

The AlliedWare Plus command line is available from local management sessions, and remote Telnet and Secure Shell management sessions. The web browser windows are available from remote web browser management sessions.

Local Manager Account

You must log on to manage the switch. This requires a valid user name and password. The switch comes with one local manager account. The user name of the account is "manager" and the default password is "friend." The user name and password are case sensitive. This account gives you access to all management modes and commands.

The default manager account is referred to as "local" because the switch authenticates the user name and password itself. If more manager accounts are needed, you can add up to eight more local manager accounts. For instructions, refer to Chapter 76, "Local Manager Accounts" on page 1289.

Another way to create more manager accounts is to transfer the task of authenticating the accounts to a RADIUS or TACACS+ server on your network. For instructions, refer to Chapter 88, "RADIUS and TACACS+ Clients" on page 1391.

The initial and default switch configuration supports up to three management sessions at one time. The number of sessions can be configured using the SERVICE MAXMANAGER command. The maximum number of sessions is 3. See "SERVICE MAXMANAGER" on page 154.

AlliedWare Plus Command Modes

The AlliedWare Plus command line interface consists of a series of modes that are arranged in the hierarchy shown in Figure 1.
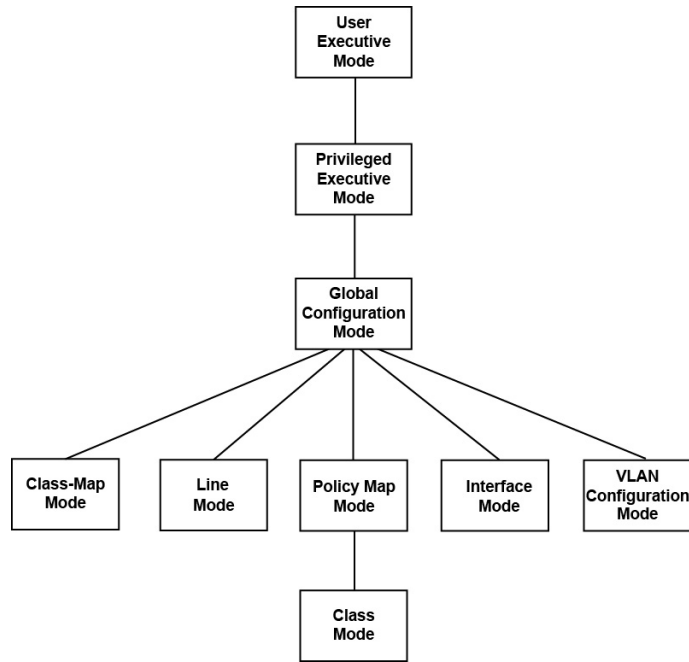
Figure 1. Command Modes

The modes have different commands and support different management functions. The only exceptions are the User Exec mode and the Privileged Exec mode. The Privileged Exec mode contains all the same commands as the User Exec mode, plus many more.

To perform a management function, you first have to move to the mode that has the appropriate commands. For instance, to configure the speeds and wiring configurations of the ports, you have to move to the Port Interface mode because the SPEED and POLARITY commands, which are used to configure the speed and wiring parameters, are stored in that mode.

Some management functions require that you perform commands from more than one mode. For instance, creating a new VLAN requires that you first go to the VLAN Configuration mode to initially create it and then to the Port Interface mode to designate the ports.

The modes, their command line prompts, and their functions are listed in Table 2 on page 50.

Note

By default, the mode prompts are prefixed with the "awplus" string.
To change this string, use the HOSTNAME command. See "What to
Configure First" on page 70.

Table 2. AlliedWare Plus Modes

Mode	Prompt	Function
User Exec mode	awplus>	❑ Displays the switch settings. ❑ Lists the files in the file system. ❑ Pings remote systems.
Privileged Exec mode	awplus#	❑ Displays the switch settings. ❑ Lists the files in the file system. ❑ Pings remote systems. ❑ Sets the date and time. ❑ Saves the current configuration. ❑ Downloads new versions of the management software. ❑ Restores the default settings. ❑ Renames files in the file system. ❑ Resets the switch.
Global Configuration mode	awplus (config)#	❑ Creates classifiers and access control lists. ❑ Creates encryption keys for remote HTTPS and SSH management. ❑ Activates and deactivates 802.1x port-based network access control. ❑ Assigns a name to the switch. ❑ Configures IGMP snooping. ❑ Sets the MAC address table aging timer. ❑ Enters static MAC addresses. ❑ Specifies the IP address of an SNTP server. ❑ Configures the RADIUS client. ❑ Sets the console timer.

Table 2. AlliedWare Plus Modes (Continued)

Mode	Prompt	Function
Console Line mode	awplus (config-line)#	❒ Sets the session timer for local management sessions. ❒ Activates and deactivates remote manager authentication.
Virtual Terminal Line mode	awplus (config-line)#	❒ Sets the session timers for remote Telnet and SSH management sessions. ❒ Activates and deactivates remote manager authentication.
Interface mode	awplus (config-if)#	❒ Configures port settings. ❒ Disables and enables ports. ❒ Configures the port mirror. ❒ Configures 802.1x port-based network access control. ❒ Creates static port trunks. ❒ Sets the load distribution method for static port trunks. ❒ Adds and removes ports from VLANs. ❒ Creates Quality of Service policies.
VLAN Configuration mode	awplus (config-vlan)#	❒ Creates VLANs.
Civic Location mode	awplus (config_civic)#	❒ Creates optional LLDP-MED civic location entries.
Coordinate Location mode	awplus (config_coord)#	❒ Creates optional LLDP-MED coordinate location entries.

Moving Down the Hierarchy

To move down the mode hierarchy, you have to step through each mode in sequence. Skipping modes is not permitted.

Each mode has a different command. For instance, to move from the User Exec mode to the Privileged Exec mode, you use the ENABLE command. Some commands, like the INTERFACE PORT command, which is used to enter the Port Interface mode, require a value, such as a port number, a VLAN ID or a port trunk ID.

ENABLE Command

You use this command to move from the User Exec mode to the Privileged Exec mode. The format of the command is:

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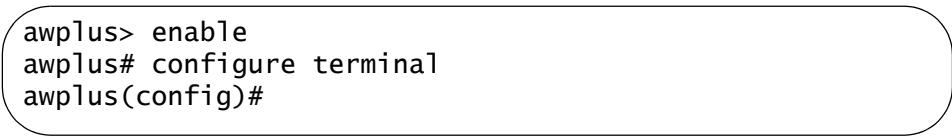
```
awplus> enable
awplus#
```

Figure 2. ENABLE Command

CONFIGURE TERMINAL Command

You use this command to move from the Privileged Exec mode to the Global Configuration mode. The format of the command is:

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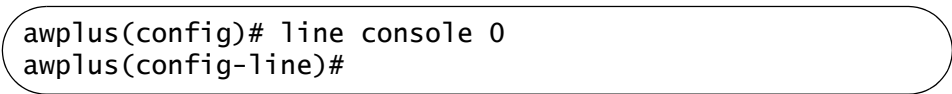
```
awplus> enable
awplus# configure terminal
awplus(config)#
```

Figure 3. CONFIGURE TERMINAL Command

LINE CONSOLE 0 Command

You use this command to move from the Global Configuration mode to the Console Line mode to set the management session timer and to activate or deactivate remote authentication for local management sessions. The mode is also used to set the baud rate of the terminal port. The format of the command is:

```
line console 0
```

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

Figure 4. LINE CONSOLE Command

LINE VTY Command

You use this command to move from the Global Configuration mode to the Virtual Terminal Line mode to set the management session timer and to activate or deactivate remote authentication of manager accounts. The format of the command is:

```
line vty line_id
```

The range of the LINE_ID parameter is 0 to 9. For information on the VTY lines, refer to "VTY Lines" on page 69. This example enters the Virtual Terminal Line mode for VTY line 2:

```
awplus(config)# line vty 2
awplus(config-line)#
```

Figure 5. LINE VTY Command

INTERFACE Command - Dynamic Port Trunk

You use this command to move from the Global Configuration mode to the Dynamic Port Trunk Interface mode, to change the load distribution methods of static port trunks. You specify a trunk by its name of "po" followed by its ID number. You can specify only one static port trunk at a time. The format of the command is:

```
interface trunk_name
```

This example enters the Port Trunk Interface mode for trunk ID 5:

```
awplus(config)# interface po5
awplus(config-if)#
```

Figure 6. INTERFACE TRUNK Command

INTERFACE Command - Ports

You use this command to move from the Global Configuration mode to the Interface mode where you configure the parameter settings of the ports and add ports to VLANs and Quality of Service policies. The format of the command is:

```
interface port
```

This example enters the Port Interface mode for port 21.

```
awplus(config)# interface port1.0.21
awplus(config-if)#
```

Figure 7. INTERFACE PORT Command - Single Port

You can configure more than one port at a time. This example enters the Port Interface mode for ports 11 to 15 and 22.

```
awplus(config)# interface port1.0.11-port1.0.15,port1.0.22
awplus(config-if)#
```

Figure 8. INTERFACE PORT Command - Multiple Ports

The INTERFACE PORT command is also located in the Port Interface mode itself, so that you do not have to return to the Global Configuration mode to configure different ports. This example moves from the current Port Interface mode to the Port Interface mode for ports 7 and 10.

```
awplus(config-if)# interface port1.0.7,port1.0.10
awplus(config-if)#
```

Figure 9. INTERFACE PORT Command - Moving Between Port Interface Modes

INTERFACE Command - Static Port Trunk

You use this command to move from the Global Configuration mode to the Static Port Trunk Interface mode, to change the load distribution methods of static port trunks. You specify a trunk by its name of "sa" followed by its ID number. You can specify only one static port trunk at a time. The format of the command is:

`interface trunk_name`

This example enters the Static Port Trunk Interface mode for trunk ID 2:

```
awplus(config)# interface sa2
awplus(config-if)#
```

Figure 10. INTERFACE TRUNK Command

INTERFACE VLAN Command

You use this command to move from the Global Configuration mode to the VLAN Interface mode to assign the switch a management IP address. The format of the command is:

`interface vlanvid`

The VID parameter is the ID of an existing VLAN on the switch. This example enters the VLAN Interface mode for a VLAN that has the VID 12:

```
awplus(config)# interface vlan12
awplus(config-if)#
```

Figure 11. INTERFACE VLAN Command

> **Note**
> A VLAN must be identified in this command by its VID and not by its name.

VLAN DATABASE Command

You use this command to move from the Global Configuration mode to the VLAN Configuration mode, which has the commands for creating VLANs. The format of the command is:

```
vlan database
```

```
awplus(config)# vlan database
awplus(config-vlan)#
```

Figure 12. VLAN DATABASE Command

LOCATION CIVIC-LOCATION Command

You use this command to move from the Global Configuration mode to the Civic Location mode, to create LLDP civic location entries. The format of the command is:

```
location civic-location id_number
```

This example assigns the ID number 16 to a new LLDP civic location entry:

```
awplus(config)# location civic-location 16
awplus(config-civic)#
```

Figure 13. LLDP LOCATION CIVIC-LOCATION Command

LOCATION COORD-LOCATION Command

You use this command to move from the Global Configuration mode to the Coordinate Location mode, to create LLDP coordinate location entries. The format of the command is:

```
location coord-location id_number
```

This example assigns the ID number 8 to a new LLDP coordinate location entry:

```
awplus(config)# location coord-location 8
awplus(config-coord)#
```

Figure 14. LLDP LOCATION COORD-LOCATION Command

Moving Up the Hierarchy

There are four commands for moving up the mode hierarchy. They are the EXIT, QUIT, END and DISABLE commands.

EXIT and QUIT Commands

These commands, which are functionally identical, are found in nearly all the modes. They move you up one level in the hierarchy, as illustrated in Figure 15.
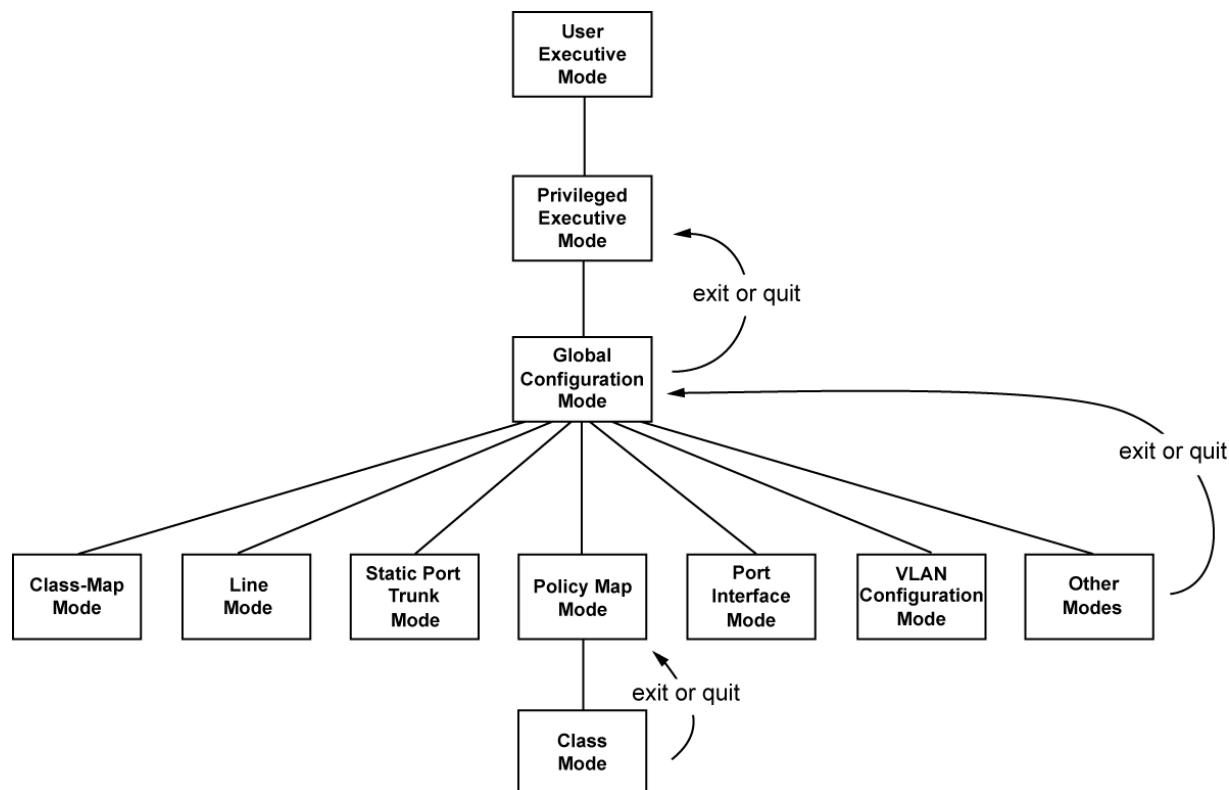
Figure 15. Moving Up One Mode with the EXIT and QUIT Command

END Command

After you have configured a feature, you may want to return to the Privileged Exec mode to verify your changes with the appropriate SHOW command. You can step back through the modes one at a time with the EXIT or QUIT command. However, the END command is more convenient because it moves you directly to the Privileged Exec mode from any mode below the Global Configuration mode.

56
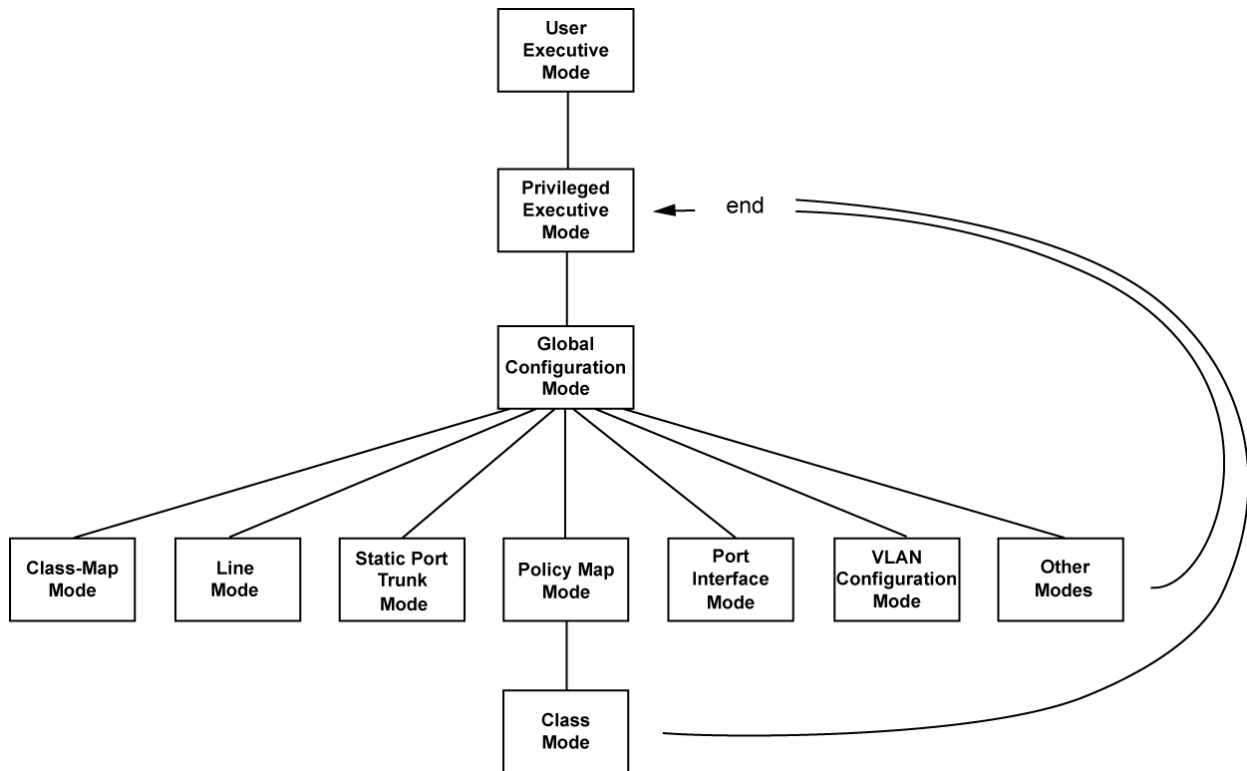
Figure 16. Returning to the Privileged Exec Mode with the END Command

DISABLE Command

To return to the User Exec mode from the Privileged Exec mode, use the DISABLE command.
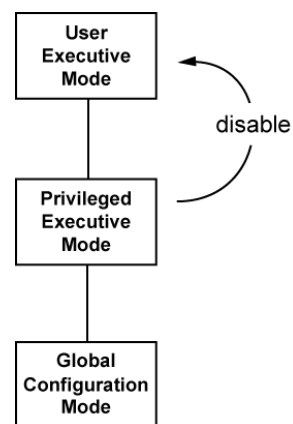
Figure 17. Returning to the User Exec Mode with the DISABLE Command

Port Numbers in Commands

The ports on the switch are identified in the commands with the PORT parameter. The parameter has the format shown in Figure 18.
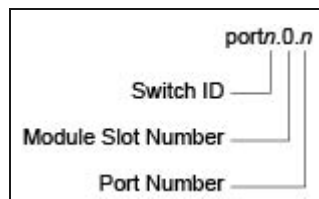
Figure 18. PORT Parameter in the Command Line Interface

The variables in the parameter are defined here:

❑ Switch ID: This number is used if the switch supports stacking. It is the switch's ID number in a stack. This number should always be 1 for AT-9000 Series switches because they do not support stacking.

❑ Module Slot ID: This number is used for modular switches that have slots for networking modules. It is used to identify the networking modules by their slot numbers. This number should always be 0 for AT-9000 Series switches because they are not modular switches.

❑ Port number: This is a port number.

> **Note**
> The correct format of the PORT parameter for AT-9000 Series switches is PORT1.0.n.

Here are a few examples of the PORT parameter. This example uses the INTERFACE PORT command to enter the Port Interface mode for ports 12 and 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12,port1.0.18
awplus(config-if)#
```

You can also specify port ranges. This example displays the port settings for ports 21 to 23:

```
awplus# show interface port1.0.21-port1.0.23
```

Note that you must include the prefix "port1.0." in the last number of a range.

You can also combine individual ports and port ranges in the same command, as illustrated in these commands, which enter the Port Interface mode for ports 5 to 11 and ports 16 and 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5-port1.0.11,port1.0.16,
port1.0.18
awplus(config-if)#
```

Combo Ports 25 to 28

Ports 25 to 28 on the AT-9000/28, AT-9000/28POE, and AT-9000/28SP Managed Layer 2 ecoSwitches are combo ports. Each combo consists of one 10/100/1000Base-T port and one SFP slot. The twisted pair ports have the letter R for Redundant as part of their port numbers on the front faceplates of the units.

Here are the guidelines to using these ports and slots:

❑ Only one port in a pair — either the twisted pair port or the companion SFP module — can be active at a time.

❑ The twisted pair port is the active port if the SFP slot is empty, or if an SFP module is installed but does not have a link to a network device.

❑ The twisted pair port automatically changes to the redundant status mode when an SFP module establishes a link with a network device.

❑ A twisted pair port automatically transitions back to the active status when a link is lost on an SFP module.

❑ A twisted pair port and an SFP module share the same configuration settings, including port settings, VLAN assignments, access control lists, and spanning tree.

❑ The only exception to shared settings is port speed. If you disable Auto-Negotiation on a twisted pair port and set the speed and duplex mode manually, the speed reverts to Auto-Negotiation when an SFP module establishes a link with an end node.

Note
These guidelines do not apply to the SFP slots on the AT-9000/52 Managed Layer 2 ecoSwitch.

Command Format

The following sections describe the command line interface features and the command syntax conventions.

Command Line Interface Features

The command line interface has these features:

- ❐ Command history - Use the up and down arrow keys.
- ❐ Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix, for example, type "sh" and the software responds with "show."
- ❐ Tab key - Pressing the Tab key fills in the rest of a keyword automatically. For example, typing "sh" and then pressing the Tab key enters "show" on the command line.

Command Formatting Conventions

This manual uses the following command format conventions:

- ❐ `screen text font` - This font illustrates the format of a command and command examples.
- ❐ [ ] - Brackets indicate optional parameters.
- ❐ | - Vertical line separates parameter options for you to choose from.
- ❐ *Italics* - Italics indicate variables you have to provide.

Command Examples

Most of the command examples in this guide start at the User Exec mode and include the navigational commands. Here is an example that creates a new VLAN called Engineering with the VID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 5 name Engineering
```

You do not have to return to the User Exec mode when you finish a management task. But it is a good idea to return to the Privileged Exec mode to confirm your changes with the appropriate SHOW command, before performing a new task.

Startup Messages

The switch generates the following series of status messages whenever it is powered on or reset. The messages can be viewed on the Console port with a terminal or a computer with a terminal emulator program.

```
CFE-NTSW-5.0.4 for BCM956218 (32bit,SP,BE,MIPS)
Build Date: Thu May 20 12:22:14 PDT 2010 (jwong@tiramisu)
Copyright (C) 2000-2008 Broadcom Corporation.

Initializing Arena.
Initializing Devices.
Board : AT9000_28SP
CPU type 0x2901A: 266MHz
Total memory: 0x8000000 bytes (128MB)

Total memory used by CFE:  0x87EB8000 - 0x87FFFBE0 (1342432)
Initialized Data:          0x87EFA324 - 0x87EFCAF0 (10188)
BSS Area:                  0x87EFCAF0 - 0x87EFDBE0 (4336)
Local Heap:                0x87EFDBE0 - 0x87FFDBE0 (1048576)
Stack Area:                0x87FFDBE0 - 0x87FFFBE0 (8192)
Text (code) segment:       0x87EB8000 - 0x87EF9B6F (269167)
Boot area (physical):      0x07E77000 - 0x07EB7000
Relocation Factor:         I:E82B8000 - D:E82B8000

Resetting uart to 9600 baud.
 Press Ctrl-C to stop auto boot..........3...2...1...
Loader:elf Filesys:raw Dev:flash0.os-Linux File:ATI Options:(null)
Loading: 0x80001000/42538636 0x8289268c/96724 Entry at 0x80230860
Starting program at 0x80230860


Starting...


          _____   ____
       /\ \           / /_____\
      /   \ \_      __/ /|  _____  |
     /     \ |     |  /  | _____  |
    /       \ \   / /    \ ___ /
   /_____/\____\ \/ /_____/

Allied Telesis Inc.Mounting Filesystems...
Starting SNMP...
Starting MainTask...
```

Figure 19. Startup Messages

```
Initializing System ................................. done!
Initializing Board .................................. done!
Initializing Serial Interface ....................... done!
Initializing Timer Library .......................... done!
Initializing IPC .................................... done!
Initializing Event Log .............................. done!
Initializing Switch Models .......................... done!
Initializing File System ............................ done!
Initializing Database ............................... done!
Initializing Configuration .......................... done!
Initializing AW+ CLI ................................ done!
Initializing Drivers ................................ done!
Initializing Port Statistics ........................ done!
Initializing Port ................................... done!
Initializing Trunk .................................. done!
Initializing Port Security .......................... done!
Initializing LACP ................................... done!
Initializing PORT VLAN .............................. done!
Initializing Port Mirroring ......................... done!
Initializing Telnet ................................. done!
Initializing Snmp Service ........................... done!
Initializing Web Service ............................ done!
Initializing Monitor ................................ done!
Initializing STP .................................... done!
Initializing SPANNING TREE .......................... done!
Initializing L2_MGMT ................................ done!
Initializing LLDP_RX ................................ done!
Initializing LLDP_TX ................................ done!
Initializing GARP ................................... done!
Initializing GARP Post Init Task .................... done!
Initializing IGMPSnoop .............................. done!
Initializing SYS_MGMT ............................... done!
Initializing SWITCH_MGMT ............................ done!
Initializing L2APP_MGMT ............................. done!
Initializing SNMP_MGMT .............................. done!
Initializing Authentication ......................... done!
Initializing TCPIP .................................. done!
Initializing Default VLAN  .......................... done!
Initializing ENCO ................................... done!
Initializing PKI .................................... done!
Initializing PortAccess ............................. done!
Initializing PAAcctRcv .............................. done!
Initializing SSH .................................... done!
Initializing IFM .................................... done!
Initializing IFMV6 .................................. done!
Initializing RTM .................................... done!
```

Figure 20. Startup Messages (continued)

63

```
Initializing FTAB ................................... done!
Initializing FTABV6 ................................. done!
Initializing ACM ................................... done!
Initializing Filter ................................ done!
Initializing L3_MGMT ............................... done!
Initializing L3APP_MGMT ............................ done!
Initializing SFLOW ................................. done!
Initializing NTP ................................... done!
Initializing CPU_HIST .............................. done!
Initializing EStacking ............................. done!
Initializing MGMT_MGMT ............................. done!

Loading configuration file "boot.cfg"  ....... done!
```

Figure 21. Startup Messages (continued)

Chapter 2

Starting a Management Session

This chapter has the following sections:

❒ "Starting a Local Management Session" on page 66

❒ "Starting a Remote Telnet or SSH Management Session" on page 68

❒ "What to Configure First" on page 70

❒ "Ending a Management Session" on page 75

> **Note**
> You must do the initial configuration of the switch from a local
> management session.

Starting a Local Management Session

To start a local management session on the switch, perform the following procedure:

1. Connect the RJ-45 connector on the management cable that comes with the switch to the Console port, as shown in Figure 22. The Console port is located on the front panels on the AT-9000/12POE, AT-9000/28, AT-9000/28POE, and AT-9000/28SP Switches and on the back panel on the AT-9000/52 Switch.
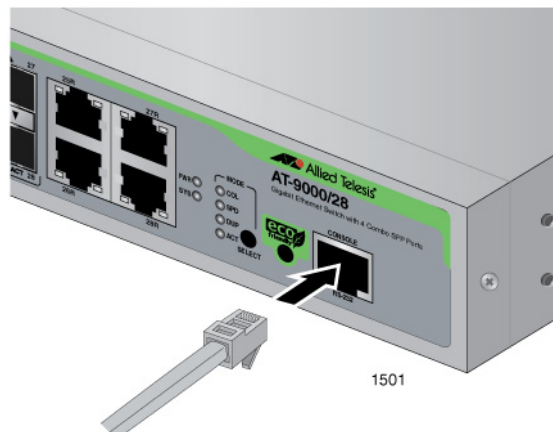
Figure 22. Connecting the Management Cable to the Console Port

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.

3. Configure the terminal or terminal emulator program as follows:

    ❒ Baud rate: 9600 bps (The baud rate of the Console Port is adjustable from 1200 to 115200 bps. The default is 9600 bps.)

    ❒ Data bits: 8

    ❒ Parity: None

    ❒ Stop bits: 1

    ❒ Flow control: None

    Note
    The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

4. Press Enter.

    You are prompted for a user name and password.

5. Enter a user name and password. If this is the initial management session of the switch, enter "manager" as the user name "friend" as the password. The user name and password are case sensitive.

The local management session has started when the AlliedWare Plus command line prompt, shown in Figure 23 is displayed.

```
awplus>
```

Figure 23. AlliedWare Plus Command Line Prompt

Starting a Remote Telnet or SSH Management Session

Here are the requirements for remote management of the switch from a Telnet or SSH client on your network:

❐ You must assign the switch a management IP address. To initially assign the switch an address, use a local management session. For instructions, refer to "What to Configure First" on page 70 or Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ The workstation that has the Telnet or SSH client must be a member of the same subnet as the management IP address on the switch, or must have access to it through routers or other Layer 3 devices.

❐ If the workstation with the Telnet or SSH client is not a member of the same subnet as the management IP address, you must also assign the switch a default gateway. This IP address needs to specify an interface on a router or other Layer 3 routing device that is the first hop to the subnet where the client resides. The default gateway must be a member of the same subnet as the management IP address. For instructions, refer to "What to Configure First" on page 70 or Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ For remote SSH management, you must create an encryption key pair and configure the SSH server on the switch. For instructions, see Chapter 82, "Secure Shell (SSH) Server" on page 1329. The factory configuration includes a default random key. When you initially connect to the switch, most SSH clients will flag the new key and ask you to accept it.

To start a remote Telnet or SSH management session, perform the following procedure:

1. In the Telnet or SSH client on your remote management workstation, enter the management IP address of the switch.

   Prompts are displayed for a user name and password.

2. Enter a user name and password of a management account on the switch. The switch comes with one management account. The user name is "manager" and the password is "friend". User names and passwords are case sensitive.

   The management session starts and the command line interface prompt is displayed, as shown in Figure 23 on page 67.

VTY Lines

The switch has ten VTY (virtual teletypewriter) lines. Each line supports one remote Telnet or SSH management session. The switch allocates the lines, which are numbered 0 to 9, in ascending order, beginning with line 0, as remote sessions are initiated.

The VTY lines cannot be reserved for particular remote workstations because the switch allocates them as needed. Line 0 is assigned by the switch to a new remote session if there are no other active remote sessions. Or, if there is already one active management session, a new session is assigned line 1, and so on.

You can adjust these three parameters on the individual lines:

❒ Management session timer - This timer is used by the switch to end inactive management sessions, automatically. This protects the switch from unauthorized changes to its configuration sessions should you leave your workstation unattended during a management session. For instructions on how to set this timer, refer to "Configuring the Management Session Timers" on page 124.

❒ Number of SHOW command scroll lines - You can specify the number of lines that SHOW commands display at one time on your screen. Refer to "LENGTH" on page 95 to set this parameter.

❒ Remote authentication of management accounts - You can toggle on or off remote authentication of management accounts on the individual VTY lines. Lines use local authentication when remote authentication is turned off. For background information, refer to Chapter 88, "RADIUS and TACACS+ Clients" on page 1391.

What to Configure First

Here are a few suggestions on what to configure during your initial management session of the switch. The initial management session must be a local management session from the Console port on the switch. For instructions on how to start a local management session, refer to "Starting a Local Management Session" on page 66.

Creating a Boot Configuration File

The first thing you should do is create a boot configuration file in the switch's file system and mark it as the active boot configuration file. This file is used by the switch to store your configuration changes. It should be noted that a boot configuration file contains only those parameter settings that have been changed from their default values on the unit. So, assuming the switch is just out of its shipping container, the file, when you create it, contains about 20 lines.

The quickest and easiest way to create a new boot configuration file and to designate it as the active file is with the BOOT CONFIG-FILE command, located in the Global Configuration mode. Here is the format of the command:

```
boot config-file filename.cfg
```

The name of the new boot configuration file, which is specified with the FILENAME parameter, can be from 1 to 16 alphanumeric characters, not including the extension ".cfg." The filename cannot contain spaces and the extension must be ".cfg."

Here is an example that creates a new boot configuration file called "switch1.cfg:"

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file switch1.cfg
```

When you see the message "Operation successful," the switch has created the file and marked it as the active boot configuration file. To confirm the creation of the file, return to the Global Configuration mode and enter the SHOW BOOT command:

```
awplus(config)# exit
awplus# show boot
```

Figure 24 on page 71 is an example of the display.

```
Current software: v2.2.1.1
Current boot image: v2.2.1.1
Default boot config: boot.cfg
Current boot config: switch1.cfg (file exists)
```

Figure 24. SHOW BOOT Command

The name of your new active boot configuration file is displayed in the "Current boot config" field.

Changing the Login Password

To protect the switch from unauthorized access, you should change the password of the manager account. The password is set with the USERNAME command in the Global Configuration. Here is the format of the command.

username *username* password *password*

Both the user name and the password are case sensitive. The password can consist of 1 to 16 alphanumeric characters including punctuation and printable special characters. Spaces are not permitted.

This example of the command changes the password of the manager account to "clearsky2a:

```
awplus> enable
awplus# configure terminal
awplus(config)# username manager password clearsky2a
```

Note
Write down the new password and keep it in a safe and secure location. If you forget the manager password, you cannot manage the switch if there are no other management accounts on the unit. In this case, contact Allied Telesis Technical Support for assistance.

For instructions on how to create additional management accounts, refer to Chapter 76, "Local Manager Accounts" on page 1289.

Assigning a Name to the Switch

The switch will be easier to identify if you assign it a name. The switch's name is displayed in the screen banner when you log on and replaces the "awplus" in the command line prompt.

A name is assigned to the switch with the HOSTNAME command in the Global Configuration mode. Here is the format of the command:

hostname *name*

A name can consist of up to 39 alphanumeric characters. Spaces, punctuation, special characters, and quotation marks are *not* permitted.

This example assigns the name "Engineering_sw2" to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# hostname Engineering_sw2
Engineering_sw2(config)#
```

Adding a Management IP Address

You must assign the switch a management IP address to use the features in Table 26 on page 286. Here are the requirements:

❑ The switch can have one management IPv4 address and one management IPv6 address.

❑ A management IP address must be assigned to a VLAN on the switch. It can be any VLAN, including the Default_VLAN. For background information on VLANs, refer to Chapter 47, "Port-based and Tagged VLANs" on page 717.

❑ The network devices (that is, syslog servers, TFTP servers, etc.) must be members of the same subnet as a management IP address or have access to it through the default gateway.

❑ The switch must also have a default gateway if the network devices are not members of the same subnet as the management IP address. The default gateway specifies the IP address of a router interface that represents the first hop to the subnets or networks of the network devices.

❑ A default gateway address, if needed, must be a member of the same subnet as a management IP address.

❑ The switch can have one IPv4 default gateway and one IPv6 gateway.

Note
The following examples illustrate how to assign a management IPv4 address to the switch. For instructions on how to assign an IPv6 address, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

The IP ADDRESS command in the VLAN Interface mode command adds a management IPv4 address to the switch. This example of the command assigns the management IPv4 address 149.82.112.72 and a subnet mask of 255.255.255.0 to the Default_VLAN, which has the VID 1. The switch is also assigned the default gateway 149.82.112.18:

Table 3. Adding a Management Address: Example 1

`awplus> enable`	Move to the Privileged Exec mode.
`awplus# configure terminal`	Move to the Global Configuration mode.
`awplus(config)# interface vlan1`	Use the INTERFACE VLAN command to move to the VLAN Interface mode of the Default_VLAN.
`awplus(config-if)# ip address 149.82.112.72/24`	Assign the management IPv4 address to the switch using the IP ADDRESS command. The mask is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. For example, the decimal masks 16 and 24 are equivalent to masks 255.255.0.0 and 255.255.255.0, respectively.
`awplus(config-if)# exit`	Return to the Global Configuration mode.
`awplus(config)# ip route 0.0.0.0/0 149.82.112.18`	Assign the default gateway to the switch using the IP ROUTE command.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show ip route`	Verify the new management IPv4 address and default gateway with the SHOW IP ROUTE command.

This example assigns the management IPv4 address to a new VLAN called Tech_Support, with the VID 5. The VLAN will consist of the untagged ports 5,6, and 23. The management IPv4 address and default route of the switch will be assigned by a DHCP server on the network:

Table 4. Adding a Management IP Address: Example 2

`awplus> enable`	Move to the Privileged Exec mode.
`awplus# configure terminal`	Move to the Global Configuration mode.
`awplus(config)# vlan database`	Enter the VLAN Configuration mode.
`awplus(config-if)# vlan 5 name Tech_Support`	Create the new VLAN with the VLAN command.
`awplus(config-if)# exit`	Return to the Global Configuration mode.
`awplus(config)# interface port1.0.5, port1.0.6,port1.0.23`	Enter the Port Interface mode for ports 5, 6, and 23.

Table 4. Adding a Management IP Address: Example 2

`awplus(config-if)# switchport access vlan 5`	Add the ports as untagged ports to the VLAN with the SWITCHPORT ACCESS VLAN command.
`awplus(config-if)# exit`	Return to the Global Configuration mode.
`awplus(config)# interface vlan5`	Use the INTERFACE VLAN command to move to the VLAN Interface mode of VLAN 5.
`awplus(config-if)# ip address dhcp`	Activate the DHCP client on the switch with the IP ADDRESS DHCP command.
`awplus(config-if)# end`	Return to the Global Configuration mode.
`awplus# show ip interface`	Verify the management IP address on the switch.
`awplus# show ip route`	Verify the new management IPv4 address and default gateway.

Saving Your Changes

To permanently save your changes in the active boot configuration file, use the WRITE command in the Privileged Exec mode:

```
awplus# write
```

You can also update the active configuration file with the COPY RUNNING-CONFIG STARTUP-CONFIG command, also located in the Global Configuration mode. It is just more to type.

74

Ending a Management Session

To end a management session, go to either the Privileged Exec mode or the User Exec mode. From the Privileged Exec mode, enter either the EXIT or LOGOUT to end a management session:

```
awplus# exit
```

or

```
awplus# logout
```

From the User Exec mode, enter either the EXIT or LOGOUT command to end a management session:

```
awplus> exit
```

or

```
awplus> logout
```

75

Chapter 3
Basic Command Line Management

This chapter contains the following sections:

❒ "Clearing the Screen" on page 78
❒ "Displaying the On-line Help" on page 79
❒ "Saving Your Configuration Changes" on page 81
❒ "Ending a Management Session" on page 82

77

Clearing the Screen

If your screen becomes cluttered with commands, you can start fresh by entering the CLEAR SCREEN command in the User Exec or Privileged Exec mode. If you are in a lower mode, you have to move up the mode hierarchy to one of these modes to use the command. Here is an example of the command from the Port Interface mode:

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

Displaying the On-line Help

The command line interface has an on-line help system to assist you with the commands. The help system is displayed by typing a question mark.

Typing a question mark at a command line prompt displays all the keywords in the current mode. This example displays all the keywords in the VLAN Configuration mode.

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# ?
  convert        Convert vlan
  do             To run exec commands in config mode
  end            End current mode and down to privileged mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  no             Negate a command or set its defaults
  private-vlan   Private-vlan
  quit           End current mode and down to previous mode
  vlan           Add, delete, or modify values associated
  with a single VLAN
```

Figure 25. Displaying the Keywords of a Mode

Typing a question mark after a keyword displays any additional keywords or parameters. This example displays the available parameters for the FLOWCONTROL command in the Port Interface mode.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# flowcontrol ?
  both           Flow control on send and receive
  receive        Flow control on receive
  send           Flow control on send
```

Figure 26. Displaying Subsequent Keywords of a Keyword

Note
You must type a space between the keyword and the question mark. Otherwise, the on-line help system simply displays the previous keyword.

Typing a question mark at the point in a command where a value is required displays a value's class (that is, integer, string, etc.). The example in Figure 27 on page 80 displays the class of the value for the HOSTNAME command in the Global Configuration mode.

```
awplus> enable
awplus# configure terminal
awplus(config)# hostname ?
  <STRING:sysName>
```

Figure 27. Displaying the Class of a Parameter

Saving Your Configuration Changes

To permanently save your changes to the parameter settings on the switch, you must update the active boot configuration file. This is accomplished with either the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command, both of which are found in the Privileged Exec mode. When you enter either of these commands, the switch copies its running configuration into the active boot configuration file for permanent storage.

To update the active configuration file, enter:

```
awplus# write
```

or

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

Note
Parameter changes that are not saved in the active boot configuration file are discarded when the switch is powered off or reset.

Ending a Management Session

To end a management session, go to either the Privileged Exec mode or the User Exec mode. From the Privileged Exec mode, enter either the EXIT or LOGOUT to end a management session:

```
awplus# exit
```

or

```
awplus# logout
```

From the User Exec mode, enter either the EXIT or LOGOUT command to end a management session:

```
awplus> exit
```

or

awplus> logout

82

Chapter 4

Basic Command Line Management Commands

The basic command line commands are summarized in Table 5.

Table 5. Basic Command Line Commands

Command	Mode	Description
"? (Question Mark Key)" on page 85	All modes	Displays the on-line help.
"CLEAR SCREEN" on page 87	User Exec and Privileged Exec	Clears the screen.
"CONFIGURE TERMINAL" on page 88	Privileged Exec	Moves you from the Privileged Exec mode to the Global Configuration mode.
"COPY RUNNING-CONFIG STARTUP-CONFIG" on page 89	Privileged Exec	Updates the active boot configuration file with the current settings from the switch.
"DISABLE" on page 90	Privileged Exec	Returns you to the User Exec mode from the Privileged Exec mode.
"DO" on page 91	Global Configuration	Performs Privileged Exec mode commands from the Global Configuration mode.
"ENABLE" on page 92	User Exec	Moves you from the User Exec mode to the Privileged Exec mode.
"END" on page 93	All modes below the Global Configuration mode	Returns you to the Privileged Exec mode.
"EXIT" on page 94	All modes except the User Exec and Privileged Exec	Moves you up one mode.
"LENGTH" on page 95	Console Line and Virtual Terminal Line	Specifies the maximum number of lines the SHOW commands display at one time on the screen.
"LOGOUT" on page 97	User Exec	Ends a management session.

83

Table 5. Basic Command Line Commands (Continued)

Command	Mode	Description
"QUIT" on page 98	All modes except the User Exec and Privileged Exec	Moves you up one mode.
"WRITE" on page 99	Privileged Exec	Updates the active boot configuration file with the current settings of the switch.

? (Question Mark Key)

Syntax

?

Parameters

None

Modes

All modes

Description

Use the question mark key to display on-line help messages. Typing the key at different points in a command displays different messages:

❒ Typing "?" at a command line prompt displays all the keywords in the current mode.

❒ Typing "?" after a keyword displays the available parameters.

Note
You must type a space between a keyword and the question mark. Otherwise, the on-line help returns the previous keyword.

❒ Typing "?" after a keyword or parameter that requires a value displays a value's class (i.e. integer, string, etc.).

Examples

This example displays all the keywords in the Port Interface mode for port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# ?
```

This example displays the parameters for the SHOW keyword in the User Exec mode and the Privileged Exec mode:

```
awplus> enable
awplus# show ?
```

85

This example displays the class of the value for the SPANNING-TREE HELLO-TIME command in the Global Configuration mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree hello-time ?
```

CLEAR SCREEN

Syntax

```
clear screen
```

Parameters

None

Modes

User Exec and Privileged Exec modes

Description

Use this command to clear the screen.

Example

```
awplus# clear screen
```

CONFIGURE TERMINAL

Syntax

```
configure terminal
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to move from the Privileged Exec mode to the Global Configuration mode.

Example

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

88

COPY RUNNING-CONFIG STARTUP-CONFIG

Syntax

```
copy running-config startup-config
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to update the active boot configuration file with the switch's current configuration, for permanent storage. When you enter the command, the switch copies its parameter settings into the active boot configuration file. The switch saves only those parameters that are not at their default settings.

> **Note**
> Parameter changes that are not saved in the active boot configuration file are discarded when the switch is powered off or reset.

To view the name of the active boot configuration file, see "SHOW BOOT" on page 484.

This command is equivalent to "WRITE" on page 99.

Example

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

DISABLE

Syntax

```
disable
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to return to the User Exec mode from the Privileged Exec mode.

Example

The following command returns the software to the User Exec mode:

```
awplus# disable
awplus>
```

DO

Syntax

do *command*

Parameter

command
    Specifies the Privileged Exec mode command to perform.

Mode

Global Configuration mode

Description

Use this command to perform Privileged Exec mode commands from the Global Configuration mode. You may use the command to perform some, but not all, of the Privileged Exec mode commands. To view the available commands, type a question mark "?" after the DO command.

Examples

This example displays all of the Privileged Exec mode commands you may perform using the DO command in the Global Configuration mode:

awplus(config)# do ?

This example displays all of the available SHOW commands:

awplus(config)# do show ?

This example performs the SHOW INTERFACE command for port 4 from the Global Configuration mode:

awplus(config)# do show interface port1.0.4

This example pings a network device:

awplus(config)# do ping 149.11.123.45

ENABLE

Syntax

```
enable
```

Parameters

None

Mode

User Exec mode

Description

Use this command to move from the User Exec mode to the Privileged Exec mode.

Example

The following command moves the prompt from the User Exec mode to the Privileged Exec mode:

```
awplus> enable
awplus#
```

END

Syntax

end

Parameters

None

Mode

All modes below the Global Configuration mode.

Description

Use this command to return to the Privileged Exec mode.

Example

The following command returns the prompt to the Privileged Exec mode:

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

EXIT

Syntax

```
exit
```

Parameters

None

Mode

All modes

Description

Use this command to move down one mode in the mode hierarchy in all modes except the User Exec and Privileged Exec modes. Using the EXIT command in the User Exec and Privileged Exec modes terminates the management session.

Example

The following example moves the prompt from the Global Configuration mode to the Privileged Exec mode:

```
awplus(config)# exit
awplus#
```

94

LENGTH

Syntax

length *value*

Parameters

value

> Specifies the maximum number of lines that the SHOW commands display at one time on the screen. The range is 0 to 512 lines. Use the value 0 if you do not want the SHOW commands to pause.

Mode

Console Line and Virtual Terminal Line modes

Description

Use this command to specify the maximum number of lines the SHOW commands display at one time on the screen during local or remote management sessions. You can set different values for the local and remote management methods. To set this parameter for local management sessions, enter the command in the Console Line mode. To set this parameter for the ten VTY lines for remote Telnet and SSH sessions, enter the same command in the Virtual Terminal Line modes. Each VTY line can have a different setting.

The default value is 20 lines for the console port. For the VTY lines, the default value is negotiated with the VTY ports.

Examples

This example sets the maximum number of lines to 25 for local management sessions:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# length 25
```

This example sets the maximum number of lines to 15 for VTY line 0:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0
awplus(config-line)# length 15
```

95

This example returns the number of lines to the default setting for local management sessions:

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

96

LOGOUT

Syntax

```
logout
```

Parameters

None

Mode

User Exec and Privileged Exec modes

Description

Use this command to end a management session.

Note
Entering the EXIT command in either the User Exec or Privileged Exec mode also ends a management session.

Example

This example shows the sequence of commands to logout starting from the Global Configuration mode:

```
awplus(config)# exit
awplus# disable
awplus> logout
```

QUIT

Syntax

```
quit
```

Parameters

None

Mode

All modes except the User Exec and Privileged Exec modes.

Description

Use this command to move up one mode in the mode hierarchy. This command is almost identical to the EXIT command. The difference is that unlike the EXIT command, the QUIT command cannot be used to end a management session.

Example

This example uses the QUIT command to return to the Privileged Exec mode from the Global Configuration mode:

```
awplus(config)# quit
awplus#
```

WRITE

Syntax

write

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to update the active boot configuration file with the switch's current configuration, for permanent storage. When you enter the command, the switch copies its parameter settings into the active boot configuration file. The switch saves only those parameters that are not at their default settings.

> **Note**
> Parameter changes that are not saved in the active boot configuration file are discarded when the switch is powered off or reset.

To view the name of the active boot configuration file, see "SHOW BOOT" on page 484.

This command is equivalent to "COPY RUNNING-CONFIG STARTUP-CONFIG" on page 89.

Example

awplus# write

100

Chapter 5

Temperature and Fan Control Overview

Overview

The switch monitors the environmental status, such as temperature and voltage, and the status of fan modules. Checking this information helps you to identify potential hardware issues before they become problems.

To check the switch's environmental and saving energy status, and turn on and off the port LEDs, use the following commands:

❐ "ECOFRIENDLY LED" on page 106

❐ "NO ECOFRIENDLY LED" on page 107

❐ "SHOW ECOFRIENDLY" on page 108

❐ "SHOW SYSTEM ENVIRONMENT" on page 109

Displaying the System Environmental Status

The switch monitors the environmental status of the switch and any attached PSU, XEM, or expansion option. The environmental status covers information about temperatures, fans, and voltage. To display this information, go to User Exec or Privileged Exec mode and enter the command:

```
awplus# show system environment
```

Figure 28 shows an example of the information the command displays. The columns are described in "SHOW SYSTEM ENVIRONMENT" on page 109.

```
Environment Monitoring Status

------------------------------------------------------------
Switch Model: AT-9000/28POE
------------------------------------------------------------
ID  Sensor (Units)      Reading  Status
------------------------------------------------------------
 0  Temp (Degrees C)    37       Normal
 1  Fan 1 (RPM)         3467     Normal
 2  PSU 1               On       Normal
 3  PSU 2               off      off
------------------------------------------------------------
```

Figure 28. SHOW SYSTEM ENVIRONMENT Command

Note
Switches that do not contain fan controllers will not display temperature readings.

Controlling Eco-Mode LED

AlliedWare Plus products provide an Eco-Mode LED control to conserve additional power on the port LEDs. The Eco-Mode LED is an eco-friendly feature that turns off the port LEDs when they are not necessary. To enable Eco-Mode LED control, enter the command:

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

To disable Eco-Mode LED control,

```
awplus(config)# no ecofriendly led
```

Chapter 6
Temperature and Fan Control Commands

The temperature and fan control commands are summarized in Table 6.

Table 6. Temperature and Fan Control Commands

Command	Mode	Description
"ECOFRIENDLY LED" on page 106	Global Configuration	Turns off the port LEDs on the switch to save power.
"NO ECOFRIENDLY LED" on page 107	Global Configuration	Turns on the port LEDs on the switch.
"SHOW ECOFRIENDLY" on page 108	Privileged Exec	Displays the power saving status of the port LEDs.
"SHOW SYSTEM ENVIRONMENT" on page 109	Privileged Exec	Displays the environmental information for the switch, such as temperatures, voltage, and fan status.

ECOFRIENDLY LED

Syntax

`ecofriendly led`

Parameters

None

Mode

Global Configuration mode

Description

Use this command to turn off the port LEDs on the switch to save power.

Confirmation Command

"SHOW ECOFRIENDLY" on page 108

Example

`awplus# ecofriendly led`

NO ECOFRIENDLY LED

Syntax

```
no ecofriendly led
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to turn on the port LEDs on the switch.

Confirmation Command

"SHOW ECOFRIENDLY" on page 108

Example

The following command turns on the port LEDs on the switch:

```
awplus# no ecofriendly led
```

SHOW ECOFRIENDLY

Syntax

```
show ecofriendly
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the power saving status of the port LEDs. An example of the information the command displays is shown in Figure 29.

```
Front panel port LEDs: on
```

Figure 29. SHOW ECOFRIENDLY Command

Example

The following example displays the power saving status of the port LEDs:

```
awplus# show ecofriendly
```

SHOW SYSTEM ENVIRONMENT

Syntax

show system environment

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the environmental information for the switch.

Figure 30 shows an example of the information that the command displays.

```
Environment Monitoring Status

------------------------------------------------------------
Switch Model: AT-9000/28POE
------------------------------------------------------------
ID  Sensor (Units)     Reading  Status
------------------------------------------------------------
 0  Temp (Degrees C)   37       Normal
 1  Fan 1 (RPM)        3467     Normal
 2  PSU 1              On       Normal
 3  PSU 2              off      off
------------------------------------------------------------
```

Figure 30. SHOW SYSTEM ENVIRONMENT Command

The columns in the display are described here:

Table 7. SHOW SYSTEM ENVIRONMENT Command

Parameter	Description
Switch Model	Indicates a model name of the switch.
ID	Indicates the ID number of an item.
Sensor (Units)	Indicates an item on the switch, such as temperature, fan, or power supply unit (PSU).

Table 7. SHOW SYSTEM ENVIRONMENT Command

Parameter	Description
Reading	Indicates the current reading of the item.
Status	Indicates the status of the item.

Example

The following example displays environmental information for the switch:

```
awplus# show system environment
```

110

Section II
Basic Operations

This section contains the following chapters:

112

Chapter 7
Basic Switch Management

This chapter contains the following:

Adding a Name to the Switch

The switch will be easier to identify if you assign it a name. The switch displays its name in the command line prompt, in place of the default prefix "awplus."

To assign the switch a name, use the HOSTNAME command in the Global Configuration mode. A name can consist of up to 39 alphanumeric characters. Spaces, punctuation, special characters, and quotation marks are *not* permitted.

This example assigns the name Switch12 to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# hostname Switch12
Switch12(config)#
```

To remove the current name without assigning a new name, use the NO HOSTNAME command:

```
Unit2b_bld4> enable
Unit2b_bld4# configure terminal
Unit2b_bld4(config)# no hostname
awplus(config)#
```

For reference information, refer to "HOSTNAME" on page 145 and "NO HOSTNAME" on page 148.

Adding Contact and Location Information

The commands for assigning the switch contact and location information are the SNMP-SERVER CONTACT and SNMP-SERVER LOCATION commands, both of which are found in the Global Configuration mode. Here are the formats of the commands:

```
snmp-server contact contact
```

```
snmp-server location location
```

The variables can be from 1 to 255 alphanumeric characters in length. Spaces and special characters are allowed.

To view the information, use the SHOW SYSTEM command in the User Exec and Privileged Exec modes.

Here is an example that assigns the switch this contact and location information:

❑ Contact: JordanB

❑ Location: 123_Westside_Dr_room_45

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server contact JordanB
awplus(config)# snmp-server location 123_Westside_Dr_room_45
```

To remove the contact or location information without adding new information, use the NO form of the commands. This example removes the location information:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server location
```

115

Displaying Parameter Settings

To display the current parameter settings on the switch, use the SHOW RUNNING-CONFIG command in the Privileged Exec mode. The settings, which are displayed in their equivalent command line commands, are limited to just those parameters that have been changed from their default values. The information includes new settings that have yet to be saved in the active boot configuration file. Here is the command:

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

For reference information, refer to "SHOW RUNNING-CONFIG" on page 158.

Manually Setting the Date and Time

To manually set the date and time on the switch, use the CLOCK SET command in the Privileged Exec mode. Here is the format of the command:

```
clock set hh:mm:ss dd mmm yyyy
```

Here are the variables:

- ❐ *hh:mm:ss*: Use this variable to specify the hour, minute, and second for the switch's time in 24-hour format.
- ❐ *dd*: Use this variable to specify the day of the month.
- ❐ *mmm*: Use this variable to specify the month. The month is specified by its first three letters. For example, June is Jun. The first letter must be uppercase and the second and third letters lowercase.
- ❐ *yyyy*: Use this variable to specify the year. The year must be specified in four digits (for example, 2011 or 2012).

The command has to include both the date and time. This example sets the time to 4:11 pm and the date to January 4, 2011:

```
awplus> enable
awplus# clock set 16:11:0 4 Jan 2011
```

To display the date and time, use the SHOW CLOCK command in the User Exec or Privileged Exec mode.

```
awplus# show clock
```

For reference information, refer to "CLOCK SET" on page 140 and "SHOW CLOCK" on page 157.

Note
The date and time, when set manually, are not retained by the switch when it is reset or power cycled.

Pinging Network Devices

If the switch is unable to communicate with a network device, such as a syslog server or a TFTP server, you can test for an active link between the two devices by instructing the switch to send ICMP Echo Requests and to listen for replies sent back from the other device. This is accomplished with the PING command in the Privileged Exec mode.

This command instructs the switch to send ICMP Echo Requests to a network device known by the IP address 149.122.14.15:

```
awplus> enable
awplus# ping 149.122.14.15
```

The results of the ping are displayed on the screen.

> **Note**
> To send ICMP Echo Requests, the switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

> **Note**
> The switch sends the ICMP Echo Requests from the ports of the VLAN assigned the management IP address. The device the switch is pinging must be a member of that VLAN or must be accessible through routers or other Layer 3 devices.

For reference information, refer to "PING" on page 149.

118

Resetting the Switch

To reset the switch, use either the REBOOT or RELOAD command in the Privileged Exec mode. You might reset the switch if it is experiencing a problem or if you want to reconfigure its settings after designating a new active boot configuration file. The commands display a confirmation prompt.

> ⚠️ **Caution**
> The switch will not forward network traffic while it initializes its management software. Some network traffic may be lost. The reset can take from thirty seconds to two minutes, depending on the number and complexity of the commands in the active boot configuration file.

> **Note**
> Any configuration changes that have not been saved in the active boot configuration file are discarded when you reset the switch. To save your changes, use the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

To reset the switch with the REBOOT command:

```
awplus> enable
awplus# reboot

Are you sure you want to reboot the switch? (y/n) y
```

To reset the switch with the RELOAD command:

```
awplus> enable
awplus# reload

Are you sure you want to reboot the switch? (y/n) y
```

To resume managing the switch, wait for the switch to initialize its management software and then start a new management session.

For reference information, refer to "REBOOT" on page 152 and "RELOAD" on page 153.

Restoring the Default Settings to the Switch

To restore the default settings to the switch, delete or rename the active boot configuration file and then reset the unit. Without an active boot configuration file, the switch will use the default parameter settings after it initializes the management software.

⚠️ **Caution**

Restoring the default settings requires that you reset the switch. The unit will not forward network traffic while it initializes the management software. Some network traffic may be lost.

There are two ways to delete the active boot configuration file. One way is with the DELETE command in the Privileged Exec mode. Here is the format of the command:

delete *filename*.cfg

This example deletes the active boot configuration file "Sales_unit.cfg" and resets the switch:

```
awplus> enable
awplus# delete Sales_unit.cfg
awplus# reboot

reboot switch? (y/n): y
```

If you do not know the name of the active boot configuration file, you can display it with the SHOW BOOT command in the Privileged Exec mode. Figure 31 is an example of what is displayed:

```
Current software   : v1.0.0
Current boot image : v1.0.0
Default boot config: /cfg/boot.cfg
Current boot config: /cfg/switch2.cfg (file exists)
```

Figure 31. SHOW BOOT Command

The active boot configuration file is identified in the "Current boot config" field.

Another way to delete the file is with the ERASE STARTUP-CONFIG command, also in the Privileged Exec mode. The advantage of this command over the DELETE command is that you do not have to know the name of the active boot configuration file. When you enter the command, a confirmation prompt is displayed. If you enter "Y" for yes, the switch automatically deletes the active boot configuration file from the file system. Afterwards, you can reset the switch with the REBOOT command so that it restores the default settings.

Here is the sequence of commands and messages:

```
awplus> enable
awplus# erase startup-config

erase start-up config? (y/n):y
Deleting..
Successful Operation
awplus# reboot

reboot switch? (y/n): y
```

If you prefer to keep the active boot configuration file, you can rename it with the MOVE command in the Privileged Exec mode and then reset the switch. Here is the format of the MOVE command:

move *filename1*.cfg *filename2*.cfg

The FILENAME1 parameter is the name of the configuration file you want to rename. The FILENAME2 parameter is the file's new name. The extensions of the files must be ".cfg". For example, if the name of the active boot configuration file is "Sales_unit.cfg," these commands rename it to "Sales_unit_backup.cfg" and reset the switch:

```
awplus> enable
awplus# move Sales_unit.cfg Sales_unit_backup.cfg
awplus# reboot

reboot switch? (y/n): y
```

To resume managing the switch after restoring the default settings, you must establish a local management session from the Console port. Remote management is not possible because the switch will not have a management IP address.

> **Note**
> For instructions on how to create a new boot configuration file, refer to Chapter 28, "Boot Configuration Files" on page 471.

Setting the Baud Rate of the Console Port

The Console port is used for local management of the switch. To set its baud rate, use the BAUD-RATE SET command in the Global Configuration mode.

Note

If you change the baud rate of the Console port during a local management session, your session is interrupted. To resume the session you must change the speed of the terminal or the terminal emulator program to match the new speed of the serial terminal port on the switch.

Here is an example to set the baud rate of the Console port on the switch to 57600 bps:

Example 1:

```
awplus> enable
awplus# configure terminal
awplus(config-conf)# baud-rate set 57600

awplus# config
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)# line console
awplus(config-line)# speed 57600

Baud rate changed to 57600 bps.
Please change your console baud rate correspondingly.
```

To display the current settings of the Console port, use the SHOW BAUD-RATE command in the User Exec or Privileged Exec mode. Here is the command:

```
awplus# show baud-rate
```

Here is an example of the information.

```
Asynchronous Port (Console) Information:
Baud Rate .................... 57600
Parity ....................... None
Data bits .................... 8
Stop bits .................... 1
```

Figure 32. SHOW BAUD-RATE Command

Note
The baud rate is the only adjustable parameter on the Console port.

For reference information, refer to "BAUD-RATE SET" on page 139 and "SHOW BAUD-RATE" on page 156.

Configuring the Management Session Timers

You should always conclude a management session by logging off so that if you leave your workstation unattended, someone cannot use it to change the switch's configuration. If you forget to log off, the switch has management session timers that detect and log off inactive local and remote management sessions automatically. A session is deemed inactive when there is no management activity for the duration of the corresponding timer.

There are different timers for the different types of management sessions. There is one timer for local management sessions, which are conducted through the Console port, and ten timers for each supported VTY line, for remote Telnet and SSH management sessions.

The command for setting the timers is the EXEC-TIMEOUT command. You enter this command in different modes depending on the timer you want to set. The timer for local management sessions is set in the Line Console mode, which is accessed using the LINE CONSOLE 0 command from the Global Configuration mode. This example of the commands sets the timer for local management sessions on the switch to 5 minutes:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# exec-timeout 5
```

> **Note**
> The default value the EXEC-TIMEOUT command is 10 minutes.

There are ten VTY lines for remote Telnet and SSH sessions. Each remote management session uses one line. The switch automatically allocates a line when a remote session is initiated. The first remote Telnet or SSH session is allocated the VTY 0 line, the second session is allocated the VTY 1 line, and so forth.

Each VTY line has its own management session timer. The timers are set in the Virtual Terminal Line mode, which is accessed with the LINE VTY command. The format of the LINE VTY command is shown here:

```
line vty first_line_id last_line_id
```

Both the first_line_id and the last_line_id parameters have value of 0 to 9. You can specify one VTY line or a range of VTY lines. This example sets the management session timer to 8 minutes on VTY line 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 2
awplus(config-line)# exec-timeout 8
```

This example sets the management session timer to 3 minutes for all VTY lines:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0 9
awplus(config-line)# exec-timeout 3
```

125

Setting the Maximum Number of Manager Sessions

The switch supports up to three manager sessions simultaneously so that more than one person can manage the unit at a time. You set the maximum number of sessions with the SERVICE MAXMANAGER command in the Global Configuration mode. The default is three manager sessions.

This example sets the maximum number of manager sessions to three:

```
awplus> enable
awplus# configure terminal
awplus(config)# service maxmanager 3
```

For reference information, refer to "SERVICE MAXMANAGER" on page 154.

Configuring the Banners

The switch has banner messages you may use to identify the switch or to display other information about the unit. The banners are listed here:

❐ Message-of-the-day banner

❐ Login banner

❐ User Exec and Privileged Exec modes banner

❐ Display login banner

Message-of-the-day banner →
```
This unit was updated to version 2.1.1 today, May 21,
2010.


This switch is located in building 2A, wiring closet4M.
```
Login banner →

```
Login: manager
Password: ******
```

User Exec and Privileged Exec modes banner →
```
                        Sales Switch 12
```
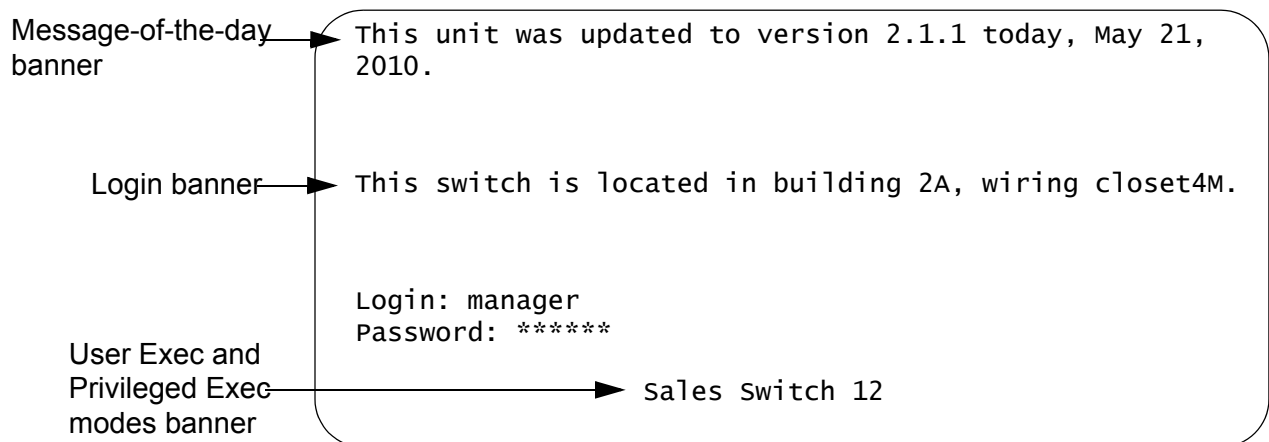
Figure 33. Banner Messages

The message-of-the-day and login banners are displayed above the login user name and password prompts of local, Telnet, and SSH management sessions. The display banner displays the contents of the login banner.

The User Exec and Privileged Exec modes banner is displayed above the command line prompts of these two modes, after you log on or whenever you use the CLEAR SCREEN command to clear the screen.

> **Note**
> The banners are not displayed in web browser management sessions.

The banner commands are:

❐ BANNER MOTD

❐ BANNER LOGIN

❐ BANNER EXEC

❐ SHOW BANNER LOGIN

127

The commands for setting the banners are located in the Global Configuration mode with the exception of the SHOW BANNER LOGIN command which you access in the Privileged Exec mode.

After you enter the BANNER EXEC, BANNER LOGIN, or BANNER MOTD command, the "Type CTRL/D to finish" prompt is displayed. When you see this message, enter the banner message. Both the BANNER MOTD and BANNER EXEC banners may be up to 256 characters, while the BANNER LOGIN banner may be up to 4,000 characters. Spaces and special characters are allowed.

After you finish entering your message, press CTRL D to return to the command prompt in the Global Configuration mode.

This example of the BANNER MOTD command assigns the switch the message-of-the-day banner in Figure 33 on page 127:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner motd
Type CTRL/D to finish
This unit was updated to version 2.1.1 today, May 21, 2010.
awplus(config)#
```

This example of the BANNER LOGIN command assigns the switch the login banner in Figure 33 on page 127:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner login
Type CTRL/D to finish
This switch is located in building 2A, wiring closet 4M.
awplus(config)#
```

Here is an example of the BANNER EXEC command:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner exec
Type CTRL/D to finish
Sales Switch 12
awplus(config)#
```

This example uses the SHOW BANNER LOGIN command to display the contents of the BANNER LOGIN file:

```
awplus> enable
awplus# configure terminal
awplus(config)# show banner login
```

To remove messages without assigning new messages, use the NO versions of the commands. This example removes the message-of-the-day banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# no banner motd
```

This example removes the login banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# no banner login
```

This example removes the User Exec and Privileged Exec modes banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# no banner exec
```

Chapter 8

Basic Switch Management Commands

The basic switch management commands are summarized in Table 8.

Table 8. Basic Switch Management Commands

Command	Mode	Description
"BANNER EXEC" on page 133	Global Configuration	Creates a User Exec and Privileged Exec modes banner.
"BANNER LOGIN" on page 135	Global Configuration	Creates a login banner.
"BANNER MOTD" on page 137	Global Configuration	Creates a message-of-the-day banner.
"BAUD-RATE SET" on page 139	Line Console	Configures the baud rate of the serial terminal port on the switch.
"CLOCK SET" on page 140	Privileged Exec	Manually sets the date and time.
"ERASE STARTUP-CONFIG" on page 141	Privileged Exec	Restores the default settings to all the parameter settings on the switch.
"EXEC-TIMEOUT" on page 142	Line Console	Sets the console timer which is used to end inactive management sessions.
"HELP" on page 144	All	Displays how to use the on-line help system.
"HOSTNAME" on page 145	Global Configuration	Assigns a name to the switch.
"LINE CONSOLE" on page 146	Global Configuration	Enters the Line Console mode.
"LINE VTY" on page 147	Global Configuration	Enters the Virtual Terminal Line mode for a VTY line.
"NO HOSTNAME" on page 148	Global Configuration	Deletes the switch's name without assigning a new name.
"PING" on page 149	User Exec and Privileged Exec	Instructs the switch to ping another network device.
"PING IPv6" on page 151	User Exec and Privileged Exec	Instructs the switch to ping another IPv6 network device.

Table 8. Basic Switch Management Commands

Command	Mode	Description
"REBOOT" on page 152	Privileged Exec	Resets the switch.
"RELOAD" on page 153	Privileged Exec	Resets the switch.
"SERVICE MAXMANAGER" on page 154	Global Configuration	Sets the maximum number of permitted manager sessions.
"SHOW BANNER LOGIN" on page 155	Privileged Exec	Displays the banner set with the BANNER LOGIN command.
"SHOW BAUD-RATE" on page 156	Global Configuration	Displays the settings of the Console port.
"SHOW CLOCK" on page 157	User Exec and Privileged Exec	Displays the date and time.
"SHOW RUNNING-CONFIG" on page 158	Privileged Exec	Displays all of the settings on the switch, including those that have not yet been saved in the active boot configuration file.
"SHOW SWITCH" on page 159	Privileged Exec	Displays general information about the switch.
"SHOW SYSTEM" on page 161	User Exec	Displays general information about the switch.
"SHOW SYSTEM SERIALNUMBER" on page 162	User Exec and Privileged Exec	Displays the serial number of the switch.
"SHOW USERS" on page 163	Privileged Exec	Displays the managers who are currently logged on the switch.
"SHOW VERSION" on page 165	User Exec and Privileged Exec	Displays the version number and build date of the management software.
"SNMP-SERVER CONTACT" on page 166	Global Configuration	Adds contact information to the switch.
"SNMP-SERVER LOCATION" on page 167	Global Configuration	Adds location information to the switch.
"SYSTEM TERRITORY" on page 168	Global Configuration	Specifies the territory of the switch.

BANNER EXEC

Syntax

```
banner exec
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to create a banner for the User Exec and Privilege Exec modes. The message is displayed above the command line prompt when you log on or clear the screen with the CLEAR SCREEN command, in local, Telnet, and SSH management sessions.

After you enter the command, the "Type CTRL/D to finish" prompt is displayed. Enter a banner message of up to 256 characters. Spaces and special characters are allowed. When you are finished, press CTRL D.

To remove the banner, use the NO version of this command, NO BANNER EXEC.

> **Note**
> Web browser management sessions do not display this banner.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example creates the banner "Production Switch 1P" for the User Exec and Privileged Exec modes:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner exec
Type CNTL/D to finish
Production Switch 1P
```

133

This example deletes the banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# no banner exec
```

BANNER LOGIN

Syntax

```
banner login
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to configure the login banner. The message is displayed prior to the login user name and password prompts for local, Telnet, and SSH management sessions. If the switch also has a message-of-the-day banner, this message is displayed after the login banner.

After you enter the command, the "Type CTRL/D to finish" prompt is displayed on your screen. Enter a login message of up to 4,000 characters. Spaces and special characters are allowed. When you are finished, press CTRL D.

To remove the login banner, use the NO version of this command, NO BANNER LOGIN.

> **Note**
> Web browser management sessions do not display the login banner.

Confirmation Command

"SHOW BANNER LOGIN" on page 155

Examples

This example creates a login banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner login
Type CTRL/D to finish
This switch is located in building B on the second floor,
wiring closet 2B.
awplus(config)#
```

This example removes the login banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# no banner login
```

BANNER MOTD

Syntax

```
banner motd
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to create a message-of-the-day banner. The message is displayed prior to the login user name and password prompts for local, Telnet, and SSH management sessions. If the switch also has a login banner, this message is displayed before the message-of-the-day banner.

After you enter the command, the "Type CTRL/D to finish" prompt is displayed. Enter a message-of-the-day banner of up to 256 characters. Spaces and special characters are allowed. When you are finished, press CTRL D.

To remove the message-of-the-day banner, use the NO version of this command, NO BANNER MOTD.

> **Note**
> Web browser management sessions do not display the message-of-the-day banner.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example create a message-of-the-day banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner motd
Type CTRL/D to finish
This switch was updated to the latest software on May 23,
2010.
```

This example removes the message-of-the-day banner:

```
awplus> enable
awplus# configure terminal
awplus(config)# no banner motd
```

BAUD-RATE SET

Syntax

```
baud-rate set 1200|2400|4800|9600|19200|38400|57600|115200
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to set the baud rate of the Console port, which is used for local management sessions of the switch.

Note

If you change the baud rate of the serial terminal port during a local management session, your session will be interrupted. To resume the session you must change the speed of your terminal or the terminal emulator program to match the new speed of the serial terminal port on the switch.

Confirmation Command

"SHOW BAUD-RATE" on page 156

Example

This example sets the baud rate of the Console port to 19200 bps:

```
awplus> enable
awplus# configure terminal
awplus(config)# baud-rate set 19200
```

139

CLOCK SET

Syntax

clock set *hh:mm:ss dd mmm yyyy*

Parameters

hh:mm:ss
> Specifies the hour, minute, and second for the switch's time in 24-hour format.

dd
> Specifies the day of the month.

mmm
> Specifies the month. The month is specified by its first three letters. For example, June is Jun. The first letter must be uppercase and the second and third letters lowercase.

year
> Specifies the year. The year must be specified in four digits (for example, 2011 or 2012).

Mode

Privileged Exec mode

Confirmation Command

"SHOW CLOCK" on page 157

Description

Use this command to manually set the date and the time on the switch. The command must include both the date and the time.

Note
When set manually the date and time are not retained by the switch when it is reset or powered off.

Example

This example sets the time and date to 2:15 pm, April 7, 2011:

```
awplus> enable
awplus# clock set 14:15:0 7 Apr 2011
```

140

ERASE STARTUP-CONFIG

Syntax

```
erase startup-config
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to delete the active boot configuration file to restore the default settings to all the parameters on the switch. After entering this command, enter the REBOOT command to reset the switch and restore the default settings.

⚠️ **Caution**
The switch will not forward network traffic while it initializes its management software. Some network traffic may be lost.

To resume managing the switch after restoring the default settings, you must establish a local management session from the Console port. Remote management is not possible because the switch will not have a management IP address.

Note
For instructions on how to create a new boot configuration file, refer to Chapter 28, "Boot Configuration Files" on page 471.

Example

The following command deletes the active boot configuration file and restores the default settings to all the parameters on the switch.

```
awplus> enable
awplus# erase startup-config

erase start-up config? (y/n):y
Deleting..
Successful Operation
awplus# reboot
```

EXEC-TIMEOUT

Syntax

```
exec-timeout value
```

Parameters

exec-timeout
>   Specifies the session timer in minutes. The range is 0 to 35,791 minutes. The default value is 10 minutes.

Mode

Line Console and Virtual Terminal Line modes

Description

Use this command to set the management session timers. The timers are used by the switch to end inactive management sessions to protect against unauthorized changes should you leave your management station unattended during a management session. A management session is deemed inactive by the switch if there is no management activity for the duration of a timer.

Local management sessions, which are conducted through the Console port on the switch, and remote Telnet and SSH sessions have different timers. The timer for local management sessions is set in the Line Console mode. The timers for remote Telnet and SSH sessions are set in the Virtual Terminal Line mode. There is a different timer for each of the ten VTY lines for remote Telnet and SSH sessions.

Confirmation Commands

"SHOW SWITCH" on page 159 and "SHOW RUNNING-CONFIG" on page 158

Examples

This example sets the session timer for local management sessions to 15 minutes:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# exec-timeout 15
```

This example sets the session timer for the first (vty 0) Telnet or SSH session to 5 minutes:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0
awplus(config-line)# exec-timeout 5
```

143

HELP

Syntax

```
help
```

Parameters

None

Mode

All modes

Description

Use this command to learn how to use on-line help. Entering this command at a command line displays how to use the on-line help system. See Figure 34 for the description displayed on the screen.

```
    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?').
```

Figure 34. HELP Command

Example

This example displays the HELP command:

```
awplus# help
```

144

HOSTNAME

Syntax

```
hostname name
```

Parameters

name

Specifies a name of up to 39 alphanumeric characters for the switch. Spaces, punctuation, special characters, and quotation marks are *not* permitted.

Mode

Global Configuration mode

Description

Use this command to assign the switch a name. The switch displays the name in the command line prompt, in place of the default prefix "awplus."

Example

This example assigns the name "Sw_Sales" to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# hostname Sw_Sales
Sw_Sales(config)#
```

LINE CONSOLE

Syntax

```
line console 0
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enter the Line Console mode to set the session timer and to activate or deactivate remote authentication for local management sessions.

Example

The following example enters the Line Console mode to set the session timer and to activate or deactivate remote authentication for local management sessions:

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

LINE VTY

Syntax

```
line vty first_line_id [last_line_id]
```

Parameters

first_line_id
> Specifies the number of a VTY line. The range is 0 to 9.

last_line_id
> Specifies the number of a VTY line. The range is 0 to 9. This is an optional parameter.

Mode

Global Configuration mode

Description

Use this command to enter the Virtual Terminal Line mode for a VTY line or a range of VTY lines, to set the session timer or to activate or deactivate remote authentication for Telnet or SSH management sessions.

Refer to "EXEC-TIMEOUT" on page 142 to set session timeout values and "LOGIN AUTHENTICATION" on page 1417 to activate remote authentication.

Examples

This example enters the Virtual Terminal Line mode for VTY line 0:

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

This example enters the Virtual Terminal Line mode for all VTY lines:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0 9
awplus(config-line)#
```

NO HOSTNAME

Syntax

no hostname

Parameters

None

Mode

Global Configuration mode

Description

Use this command to delete the switch's name without assigning a new name.

Example

This example deletes the current name of the switch without assigning a new value:

```
Bld2_Shipping> enable
Bld2_Shipping# configure terminal
Bld2_Shipping(config)# no hostname
awplus#(config)
```

148

PING

Syntax

ping *ipaddress|hostname*

Parameters

ipaddress
> Specifies the IP address of the network device to receive the ICMP Echo Requests from the switch. You can specify only one IP address.

hostname
> Specifies the host name of the network device to receive the ICMP Echo Requests from the switch. You can specify only one host name.

Modes

Privileged Exec mode

Description

Use this command to instruct the switch to send ICMP Echo Requests to a network device with an IPv4 address. You can use the command to determine whether there is an active link between the switch and another network device, such as a RADIUS server or a Telnet client, or to troubleshoot communication problems. To ping an IPv6 address, see "PING IPv6" on page 151.

In order to specify the host name parameter, the switch needs a connection to a name server. To accomplish this, the switch can obtain a name server automatically with DHCP. See "IP ADDRESS DHCP" on page 304 for information about how to set the switch to DHCP.

Note
To send ICMP Echo Requests the switch must be configured with a management IP address. For background information, refer to

Note
The switch sends the ICMP Echo Requests from the ports of the VLAN assigned the management IP address. The device the switch is pinging must be a member of that VLAN or must be accessible through routers or other Layer 3 devices.

Example

This command instructs the switch to ping a network device with the IP address 149.122.14.15:

```
awplus> enable
awplus# ping 149.122.14.15
```

The results of the ping are displayed on the screen.

PING IPv6

Syntax

```
ping ipv6 <ipv6-address> repeat <1-99> size <36-18024>
```

Parameters

ipv6-address

Indicates the destination IPv6 address. The IPv6 address uses the format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where N is a hexadecimal digit from 0 to F. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

12c4:421e:09a8:0000:0000:0000:00a4:1c50

12c4:421e:09a8::a4:1c50 X:X::X:X

repeat <1-99>

Specifies the number of times the ping is sent. The default is 4 times.

size *<36-18024>*

Indicates the packet size, in bytes, that are sent to the destination IPv6 address. The packet size excludes the 8 byte ICMP header. The default is 56 bytes. The range is 36 to 18,024 bytes.

Mode

User Exec and Privileged Exec modes

Description

Use this command to instruct the switch to send ICMP Echo Requests to an IPv6 host.

Example

The following example sends 37 data bytes in an ICMP Echo Request to IPv6 address 2001:0db8::a2 for a total of 12 times:

```
awplus> enable
awplus# ping ipv6 2001:0db8::a2 repeat 12 size 37
```

151

REBOOT

Syntax

```
reboot
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to reset the switch. You might reset the unit if it is experiencing a problem or if you want to reconfigure its settings after you designate a new active boot configuration file.This command is identical to "RELOAD" on page 153. The command displays a confirmation prompt.

> ⚠️ **Caution**
> The switch does not forward network traffic while it initializes its management software. Some network traffic may be lost. The reset can take from 10 seconds to two minutes, depending on the number and complexity of the commands in the active boot configuration file.

> **Note**
> The switch discards any configuration changes that have not been saved in its active boot configuration file. To save your changes, enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command before resetting the switch. For instructions, refer to "WRITE" on page 99 or "COPY RUNNING-CONFIG STARTUP-CONFIG" on page 89.

To resume managing the switch, wait for the switch to initialize the management software and then start a new management session.

Example

The following command resets the switch:

```
awplus> enable
awplus# reboot

Are you sure you want to reboot the switch? (y/n): y
```

RELOAD

Syntax

```
reload
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to reset the switch. You might reset the unit if it is experiencing a problem or if you want to reconfigure its settings after you designate a new active boot configuration file. This command is identical to "REBOOT" on page 152. The command displays a confirmation prompt.

⚠️ **Caution**
The switch does not forward network traffic while it initializes its management software. Some network traffic may be lost. The reset can take from 10 seconds to 2 minutes, depending on the number and complexity of the commands in the active boot configuration file.

Note
The switch discards any configuration changes that have not been saved in its active boot configuration file. To save your changes, enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command before resetting the switch. For instructions, refer to "WRITE" on page 99 or "COPY RUNNING-CONFIG STARTUP-CONFIG" on page 89.

To resume managing the switch, wait for the switch to initialize the management software and then start a new management session.

Example

The following example resets the switch:

```
awplus> enable
awplus# reload

reboot switch? (y/n): y
```

SERVICE MAXMANAGER

Syntax

```
service maxmanager value
```

Parameters

value

Specifies the maximum number of manager sessions the switch will allow at one time. The range is 1 to 3. The default is 3.

Mode

Global Configuration mode

Description

Use this command to set the maximum number of manager sessions that can be open on the switch simultaneously. This feature makes it possible for more than one person to manage the unit at one time. The range is one to three manager sessions, with the default, three manager sessions.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the maximum number of manager sessions to two:

```
awplus> enable
awplus# configure terminal
awplus(config)# service maxmanager 2
```

SHOW BANNER LOGIN

Syntax

```
show banner login
```

Parameters
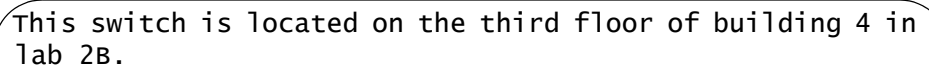
None

Mode

Privileged Exec mode

Description

Use this command to display the contents of the banner login file configured with the BANNER LOGIN command. A sample of the display is shown below.

```
This switch is located on the third floor of building 4 in
lab 2B.
```

Figure 35. SHOW BANNER LOGIN Command

Example

This example displays the contents of the banner login file configured with the BANNER LOGIN command:

```
awplus> enable
awplus# show banner login
```

SHOW BAUD-RATE

Syntax

```
show baud-rate
```

Parameters
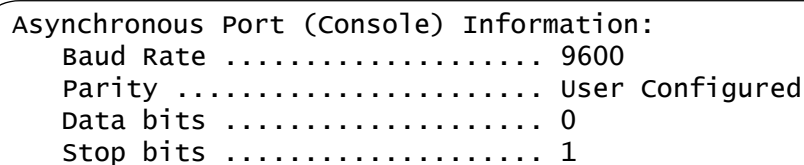
None

Mode

User Exec mode and Privileged Exec mode

Description

Use this command to display the settings of the Console port, used for local management sessions of the switch. Here is an example of the information.

```
Asynchronous Port (Console) Information:
   Baud Rate .................... 9600
   Parity ....................... User Configured
   Data bits .................... 0
   Stop bits .................... 1
```

Figure 36. SHOW BAUD-RATE Command

To set the baud rate, refer to "BAUD-RATE SET" on page 139.

Note
The baud rate is the only adjustable parameter on the Console port.

Example

This example displays the settings of the console port:

```
awplus# show baud-rate
```

156

SHOW CLOCK

Syntax

show clock

Parameters

None

Modes

User Exec mode

Description

Use this command to display the system's current date and time.

Example

This example displays the system's current date and time:

awplus# show clock

SHOW RUNNING-CONFIG

Syntax

```
show running-config
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the settings of the switch, in their equivalent command line commands.

The command displays only the settings that have been changed from their default values and includes those values that have not yet been saved in the active boot configuration file. Parameters at their default settings are not included in the running configuration file.

To display the port configuration settings, see "SHOW RUNNING-CONFIG INTERFACE" on page 232.

Example

This example displays the switch settings:

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

SHOW SWITCH

Syntax

show switch

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to view the information in Figure 37.

```
Switch Information:
Application Software Version ......... v1.0.0
Application Software Build date ...... May 2010 10:24:12
MAC Address .......................... 00:15:77:cc:e2:42
Console Disconnect Timer Interval .... 10 minute(s)
Telnet Server status ................. Enabled
MAC address aging time ............... 300 second(s)
Multicast Mode ....................... Unknown
```

Figure 37. SHOW SWITCH Command

The fields are described in Table 9.

Table 9. SHOW SWITCH Command

Parameter	Description
Application Software Version	The version number of the management software.
Application Software Build Date	The date and time when Allied Telesis released this version of the management software.
MAC Address	The MAC address of the switch.

159

Table 9. SHOW SWITCH Command (Continued)

Parameter	Description
Active Spanning Tree version	The active spanning tree protocol on the switch. The protocol can be STP, RSTP, or MSTP. The active spanning tree protocol is set with "SPANNING-TREE MODE STP" on page 628, "SPANNING-TREE MODE RSTP" on page 664, and "SPANNING-TREE MODE MSTP" on page 706.
Console Disconnect Timer Interval	The current setting of the console timer. The switch uses the console timer to end inactive management sessions. The switch ends management sessions if they are inactive for the length of the timer. To set the timer, refer to "EXEC-TIMEOUT" on page 142.
Telnet Server Status	The status of the Telnet server. The switch can be remotely managed from a Telnet client on your network when the server is enabled. When the server is disabled, the switch cannot be remotely managed with a Telnet client. To configure the Telnet client, refer to "SERVICE TELNET" on page 1319 and "NO SERVICE TELNET" on page 1318.
MAC Address Aging Time	The current setting of the aging timer, which the switch uses to delete inactive dynamic MAC addresses from the MAC address table. To set this value, refer to "MAC ADDRESS-TABLE AGEING-TIME" on page 356.

Example

The following example displays the switch information:

```
awplus# show switch
```

160

SHOW SYSTEM

Syntax

show system

Parameters

None

Modes

User Exec and Privileged Exec modes

Description

Use this command to view general information about the switch. Figure 38 is an example of the information.

```
Switch System StatusFri, 18 Nov 2011 00:37:26
BoardBoard NameRevSerial Number
-------------------------------------------------------------------
BaseAT-9000/28 R1S05525A090200007
-------------------------------------------------------------------

Environmental Status:Normal
Uptime:0 days 00:37:27
Bootloader version:5.1.2
Bootloader build date:June 01 2010 10:24:05

Software version:2.2.2.0
Build date:Oct 23 2011 01:40:25

Current boot config:/cfg/switch1a.cfg (file exists)
Territory:

System Name:

System Contact:

System Location:
```

Figure 38. SHOW SYSTEM Command

Example

This example displays general information about the switch:

awplus# show system

SHOW SYSTEM SERIALNUMBER

Syntax

```
show system serialnumber
```

Parameters

None

Mode

User Exec and Privileged Exec modes

Description

Use this command to display the serial number of the switch. Figure 39 is an example of the output.

```
S05525A023600001
```

Figure 39. SHOW SYSTEM SERIALNUMBER Command

Example

This example displays the system's serial number:

```
awplus# show system serialnumber
```

SHOW USERS

Syntax

```
show users
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the managers who are currently managing the switch locally through the Console port and remotely from Telnet and SSH sessions. This command does not display managers who are configuring the device with a web browser application or an SNMP application. Figure 40 displays an example of the information.

```
LineUserHost(s)IdleLocation
con0manageridle00:00:00ttyS0
vty0Brandonidle00:03:11149.112.167.29
```

Figure 40. SHOW USERS Command

The columns are described in Table 10.

Table 10. SHOW USERS Command

Parameter	Description
Line	The active management sessions. The possible designators are "con0" for a local management session and "vty" for remote Telnet and SSH sessions.
User	The login user name of the manager account.
Host(s)	This field is not applicable to the switch.

Table 10. SHOW USERS Command (Continued)

Parameter	Description
Idle	The number of hours, minutes, and seconds since the manager using the account entered a command on the switch. The value is always zero for your account because you just entered the SHOW USERS command.
Location	The network device from which the manager is accessing the switch. A device connected to the Console port is identified by "ttys0", while remote Telnet and SSH devices are identified by their IP addresses.
Priv	The privilege level of the manager account. Manager accounts with the privilege level 1 are restricted to the User Exec mode, while accounts with the level 15 can access all of the command modes.

Example

This example displays the managers who are logged on to the switch:

```
awplus# show users
```

SHOW VERSION

Syntax

show version

Parameters

None

Mode

User Exec and Privileged Exec modes

Description

Use this command to display the software version number and build date of the management software. Figure 41 displays an example of the information.

```
AlliedWare Plus (TM) 2.1.3.0 09/15/11 14:37:22


Application Build name : ats-9000-2.1.3.0.img
Application Build date : Sep 15 2011 14:37:22
Application Build type : RELEASE

Bootloader version     : 5.0.4
```

Figure 41. SHOW VERSION Command

Example

This example displays the management software version number:

awplus# show version

SNMP-SERVER CONTACT

Syntax

```
snmp-server contact contact
```

Parameters

contact
Specifies the name of the person responsible for managing the switch. The name can be up to 255 alphanumeric characters in length. Spaces and special characters are allowed.

Mode

Global Configuration mode

Description

Use this command to add contact information to the switch. The contact information is usually the name of the person who is responsible for managing the unit.

To remove the current contact information without adding a new contact, use the NO form of this command.

Confirmation Command

"SHOW SYSTEM" on page 161

Example

This example assigns the contact "JSmith_ex5441" to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server contact JSmith_ex5441
```

This example removes the current contact information:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server contact
```

SNMP-SERVER LOCATION

Syntax

```
snmp-server location location
```

Parameters

location
> Specifies the location of the switch. The location can be up to 255 alphanumeric characters. Spaces and special characters are allowed.

Mode

Global Configuration mode

Description

Use this command to add location information to the switch.

To remove the current location information without adding new information, use the NO form of this command.

Confirmation Command

"SHOW SYSTEM" on page 161

Examples

This example adds the location "Bldg5_fl2_rm201a" to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server location Bldg5_fl2_rm201a
```

This example removes the current location information:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server location
```

SYSTEM TERRITORY

Syntax

```
system territory territory
```

Parameters

territory

Specifies the territory of the switch. The switch can have only one territory. You may choose from the following:

australia

china

europe

japan

korea

nz (New Zealand)

usa

Mode

Global Configuration mode

Description

Use this command to specify the territory of the switch. The territory setting is not currently used by any of the features on the switch.

Confirmation Command

"SHOW SYSTEM" on page 161

Examples

This example sets the switch's territory to Australia:

```
awplus> enable
awplus# configure terminal
awplus(config)# system territory australia
```

This example removes the current territory information:

```
awplus> enable
awplus# configure terminal
awplus(config)# no system territory
```

Chapter 9

Port Parameters

This chapter contains the following:

Adding Descriptions

The ports will be easier to identify if you give them descriptions. The descriptions are viewed with the SHOW INTERFACE command in the Privileged Exec mode.

The command for adding descriptions is the DESCRIPTION command in the Port Interface mode. Here is the format:

```
description description
```

The DESCRIPTION parameter can be up to 80 alphanumeric characters. Spaces and special characters are allowed.

You can assign a description to more than one port at a time.

To remove the current description from a port without assigning a new description, use the NO form of this command.

This example assigns the name "printer22" to port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# description printer22
```

This example removes the current name from port 16 without assigning a new description:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# no description
```

For reference information, refer to "DESCRIPTION" on page 198.

> **Note**
> The POWER-INLINE DESCRIPTION command is used to describe powered devices that are connected to the ports. For information about this command, see "POWER-INLINE DESCRIPTION" on page 267.

Setting the Speed and Duplex Mode

The twisted pair ports on the switch can operate at 10, 100, or 1000 Mbps, in either half-duplex or full-duplex mode. You may set the speeds and duplex modes yourself or, since the ports support Auto-Negotiation, you may let the switch configure the ports automatically. The default setting for the ports is Auto-Negotiation for both speed and duplex mode.

To set the speed manually on a port or to reactivate Auto-Negotiation, use the SPEED command in the Port Interface mode. The format of the command is:

```
speed auto|10|100|1000
```

The "10" setting is for 10Mbps, the "100" for 100Mbps and the "1000" for 1000Mbps. The "auto" activates Auto-Negotiation for port speed.

The DUPLEX command, for setting the duplex mode, has this format:

```
duplex auto|half|full
```

The "half" setting is for half-duplex mode and "full" for full-duplex mode. The "auto" activates Auto-Negotiation for duplex mode.

You should review the following information before configuring the ports:

❒ Auto-Negotiation may be activated separately for speed and duplex mode on a port. For instance, you may activate Auto-Negotiation for speed on a port, but set the duplex mode manually.

❒ The 1000 Mbps setting in the SPEED command is for fiber optic modules. The twisted pair ports on the switch must be set to Auto-Negotiation to operate at 1000 Mbps.

Note

To avoid a duplex mode mismatch between switch ports and network devices, do not use duplex mode Auto-Negotiation on ports that are connected to network devices on which the duplex modes are set manually. Switch ports that are set to Auto-Negotiation default to half duplex mode if they detect that the network devices are not using Auto-Negotiation. This may result in duplex mode mismatches in which the switch ports use half duplex mode, and the network devices full duplex mode. To prevent this problem, always manually set the duplex mode on ports that are connected to network devices that are not using Auto-Negotiation.

This example sets the speeds of ports 11 and 17 to 100Mbps:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11,port1.0.17
awplus(config-if)# speed 100
```

This example configures port 1 to half-duplex:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# duplex half
```

This example configures ports 2 to 4 to 10 Mbps, full-duplex:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# speed 10
awplus(config-if)# duplex full
```

This example sets the speed on port 15 to Auto-Negotiation and the duplex mode to half duplex:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# speed auto
awplus(config-if)# duplex half
```

This example sets the speed on port 23 to 100 Mbps and the duplex mode to Auto-Negotiation:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# speed 100
awplus(config-if)# duplex auto
```

For reference information, refer to "SPEED" on page 239 and "DUPLEX" on page 200.

Setting the MDI/MDI-X Wiring Configuration

The wiring configurations of twisted pair ports that operate at 10 or 100 Mbps are MDI (medium dependent interface) and MDI-X (medium dependent interface crossover). A port on the switch and a port on a link partner must have different settings. For instance, a switch port has to be using the MDI wiring configuration if the port on its link partner is using the MDIX wiring configuration.

The command for setting the wiring configuration is the POLARITY command in the Port Interface mode. Here is the format of the command:

```
polarity auto|mdi|mdix
```

The AUTO setting activates auto-MDI/MDIX, which enables a port to detect the wiring configuration of its link partner so that it can set its wiring configuration to the opposite setting.

This example of the command configures ports 22 and 23 to the MDI wiring configuration:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22,port1.0.23
awplus(config-if)# polarity mdi
```

This example activates auto-MDI/MDIX on ports 7 to 9:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7-port1.0.9
awplus(config-if)# polarity auto
```

For reference information, refer to "POLARITY" on page 214.

Enabling or Disabling Ports

Disabling ports turns off their receivers and transmitters so that they cannot forward traffic. You might disable unused ports on the switch to protect them from unauthorized use, or if there is a problem with a cable or a network device.

To disable ports, use the SHUTDOWN command in the Port Interface mode. To enable ports again, use the NO SHUTDOWN command.

This example disables ports 1 to 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# shutdown
```

This example enables ports 17 and 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17,port1.0.22
awplus(config-if)# no shutdown
```

For reference information, refer to "SHUTDOWN" on page 237 and "NO SHUTDOWN" on page 211.

Enabling or Disabling Backpressure

Ports use backpressure during periods of packet congestion, to prevent packet overruns. They use it to stop their link partners from sending any further packets to enable them to process the packets already in their buffers.

Backpressure applies to ports that are operating in half-duplex mode at 10 or 100 Mbps. A port that is experiencing packet congestion initiates backpressure by transmitting a signal on the shared link. When the link partner detects that its own transmission has become garbled on the link, it ceases transmission, waits a random period of time, and, if the link is clear, resumes transmitting.

You can enable or disable backpressure on ports where you disabled Auto-Negotiation and set the speeds and duplex modes manually. If you enable backpressure, the default setting, a port initiates backpressure when it needs to prevent a buffer overrun from packet congestion. If you disable backpressure, a port does not use backpressure. (Ports that are set to Auto-Negotiation always use backpressure when operating in half-duplex mode at 10 or 100 Mbps.)

Backpressure is set with the BACKPRESSURE command in the Port Interface mode. In this example, ports 11 and 12 are manually set to 10 Mbps, half-duplex, with backpressure enabled:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11,port1.0.12
awplus(config-if)# speed 10
awplus(config-if)# duplex half
awplus(config-if)# backpressure on
```

In this example, port 12 is manually set to 100 Mbps, half-duplex, with backpressure disabled:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# speed 100
awplus(config-if)# duplex half
awplus(config-if)# backpressure off
```

For reference information, refer to "BACKPRESSURE" on page 194.

Enabling or Disabling Flow Control

When a port that is operating in full-duplex mode needs to temporarily stop its local or remote counterpart from sending any further packets, it initiates flow control by sending what are known as pause packets. Pause packets instruct the link partner to stop sending packets to allow the sender of the packets time to process the packets already stored in its buffers.

There are two aspects to flow control on the ports on the switch. The first is whether or not a port will issue pause packets during periods of buffer congestion. The other is whether or not a port will stop sending packets when it receives pause packets from another network device. You can control both of these aspects of flow control on the ports on the switch.

Flow control is set with the FLOWCONTROL RECEIVE command and the the FLOWCONTROL SEND command. The formats of the commands are:

```
flowcontrol send on|off
flowcontrol receive on|off
```

The FLOWCONTROL SEND command controls whether or not a port sends pause packets during periods of packet congestion. If you set it to ON, the port sends pause packets when it reaches the point of packet congestion. If you set it to OFF, the port does not send pause packets. At the default setting, the send portion of flow control is off.

The FLOWCONTROL RECEIVE command is used to control whether or not a port stops transmitting packets when it receives pause packets from its local or remote counterpart. If you set it to ON, a port stops transmitting packets when it receives pause packets. If you set it to OFF, a port does not stop transmitting packets when it receives pause packets. At the default setting, the receive portion of flow control is off.

The commands are located in the Port Interface mode. This example configures ports 12 and 13 to 100Mbps, full-duplex mode. The receive portion of flow control is disabled so that the ports ignore any pause packets that they receive from their link partners:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12,port1.0.13
awplus(config-if)# speed 100
awplus(config-if)# duplex full
awplus(config-if)# flowcontrol receive off
```

This example configures port 21 not to send pause packets during periods of packet congestion:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# speed 100
awplus(config-if)# duplex full
awplus(config-if)# flowcontrol send off
```

This example enables both the receive and send portions of flow control on port 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# flowcontrol receive on
awplus(config-if)# flowcontrol send on
```

For reference information, refer to "FLOWCONTROL" on page 204.

To disable flow control, use the NO FLOWCONTROL command in the Port Interface mode. This example disables flow control on ports 22 and 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22,port1.0.23
awplus(config-if)# no flowcontrol
```

To view the flow control settings on ports, use the SHOW FLOWCONTROL INTERFACE command in the Privilege Exec mode. Here is the format of the command:

```
show flowcontrol interface port
```

You can view just one port at a time. This example displays the flow control settings for port 4:

```
awplus# show flowcontrol interface port1.0.4
```

Here is an example of the information the command displays.

```
Port      Send      Receive    RxPause    TxPause
          admin     admin
-----     -------   -------    -------    -------
1.0.4     yes       yes        112        83
```

Figure 42. SHOW FLOWCONTROL INTERFACE Command

The columns in the table are described in "SHOW FLOWCONTROL INTERFACE" on page 219.

If flow control is not configured on a port, this message is displayed:

```
Flow control is not set on interface port1.0.2
```

Resetting Ports

If a port is experiencing a problem, you may be able to correct it with the RESET command in the Port Interface mode. This command performs a hardware reset. The port parameter settings are retained. The reset takes just a second or two to complete.

This example resets ports 16 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16,port1.0.17
awplus(config-if)# reset
```

For reference information, refer to "RESET" on page 218.

Configuring Threshold Limits for Ingress Packets

You can set threshold limits for the ingress packets on the ports. The threshold limits control the number of packets the ports accept each second. Packets that exceed the limits are discarded by the ports. You can set different limits for broadcast, multicast, and unknown unicast traffic. This feature is useful in preventing bottlenecks from forming in a network.

To assign a threshold limit on a port, use the STORM-CONTROL command in the Port Interface mode. The format is:

```
storm-control broadcast|multicast|dlf level value
```

The BROADCAST, MULTICAST and DLF parameters specify the packet type of the threshold limit. (The DLF parameter, the acronym for "database lookup failure," is for unknown unicast packets.) The VALUE parameter specifies the maximum permitted number of ingress packets per second a port will accept. The range is 0 to 33,554,431 packets.

This example sets a threshold of 5,000 packets per second for ingress broadcast packets on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# storm-control broadcast level 5000
```

This example sets a threshold of 100,000 packets per second for ingress multicast packets on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# storm-control multicast level 100000
```

This example sets a threshold of 200,000 packets per second for ingress unknown unicast packets on ports 15 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.17
awplus(config-if)# storm-control dlf level 200000
```

To remove threshold limits from the ports, use the NO STORM-CONTROL command, also in the Port Interface mode. This example removes the threshold limit for broadcast packets on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no storm-control broadcast
```

This example disables unknown unicast rate limiting on port 5, 6, and 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.6,port1.0.15
awplus(config-if)# no storm-control dlf
```

This example removes the threshold limit for multicast packets on port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no storm-control multicast
```

For reference information, refer to "STORM-CONTROL" on page 241 and "NO STORM-CONTROL" on page 213.

Displaying Threshold Limit Settings on Ports

To display the threshold settings for the ingress packets on the ports, use the SHOW STORM-CONTROL command in the Privileged Exec mode. Here is the format:

```
show storm-control [port]
```

This example of the command displays the broadcast, multicast and dif levels on ports 18:

```
awplus# show storm-control port1.0.18
```

Here is an example of the information the command displays.

```
Port        Bcastlevel    Mcastlevel    Diflevel
port1.0.18        30          100         100
```

Figure 43. SHOW STORM-CONTROL Command

The columns are described in Table 15 on page 227.

If the parameter port is not specified, the command displays the threshold settings on all the ports on the switch.

If you want to display information on multiple ports at a time, enter:

```
awplus# show storm-control port1.0.18,port1.0.20,port1.0.21
```

Here is an example of the information the command displays.

```
Port        Bcastlevel    Mcastlevel    Diflevel
port1.0.18        30          100         100
Port1.0.20       100           50         100
port1.0.21       100          100         100
```

Figure 44. SHOW STORM-CONTROL Command

Reinitializing Auto-Negotiation

If you believe that a port set to Auto-Negotiation is not using the highest possible common speed and duplex-mode between itself and a network device, you can instruction it to repeat Auto-Negotiation. This is accomplished with the RENEGOTIATE command in the Port Interface mode. The command does not have any parameters. A port must already be set to Auto-Negotiation before you can use this command.

This example prompts ports 4 and 8 to use Auto-Negotiation to renegotiate their settings with the ports on their network counterparts:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.8
awplus(config-if)# renegotiate
```

For reference information, refer to "RENEGOTIATE" on page 217.

Restoring the Default Settings

To restore the default settings on a port, use the PURGE command in the Port Interface mode. This example returns ports 12, 13 and 15 to their default settings:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12,port1.0.13,port1.0.15
awplus(config-if)# purge
```

For reference information, refer to "PURGE" on page 216.

186

Displaying Port Settings

There are several ways to display port settings. See the following:

❑ "Displaying Speed and Duplex Settings" on page 187

❑ "Displaying Port Status" on page 187

❑ "Displaying Port Configuration" on page 188

Displaying Speed and Duplex Settings

To display the speed and duplex mode settings of the ports, use the SHOW INTERFACE STATUS command in the Privileged Exec mode. Here is the format:

```
show interface [port] status
```

This example of the command displays the speed and duplex mode settings for ports 18 and 20:

```
awplus# show interface port1.0.18,port1.0.20 status
```

Here is an example of the information the command displays.

```
Port        Name      Status    Vlan  Duplex  Speed  Type
port1.0.18  Port_01   down      3     half    100    10/100/1000Base-T
port1.0.20  Port_02   up        11    auto    auto   10/100/1000Base-T
```

Figure 45. SHOW INTERFACE STATUS Command

The columns are described in Table 15 on page 227. For a description of the command, see "SHOW INTERFACE STATUS" on page 227.

Displaying Port Status

To display the current status of the ports on the switch, use the SHOW INTERFACE command in the Privileged Exec mode. Here is the format:

```
show interface [port]
```

This example displays the settings for ports 1 and 2:

```
awplus# show interface port1.0.1,port1.0.2
```

See Figure 46 on page 188 for an example of the display.

```
Interface port1.0.1
    Link is UP, administrative state is UP
    Address is 0015.77cc.e243
    index 1 mtu 9198
    SNMP link-status traps: Enabled (Suppressed in 0 sec.)
    Bandwidth 1g
        input packets 0, bytes 0, dropped 0, multicast packets 0
        output packets 0, bytes 0, multicast packets 0 broadcast packets 0
Interface port1.0.2
    Link is UP, administrative state is UP
    Address is 0015.77cc.e244
    index 2 mtu 9198
    SNMP link-status traps: Enabled (Suppressed in 0 sec.)
    Bandwidth 1g
        input packets 0, bytes 0, dropped 0, multicast packets 0
        output packets 0, bytes 0, multicast packets 0 broadcast packets 0
```

Figure 46. SHOW INTERFACE Command

The fields are described in Table 13 on page 222. For a description of the command, see "SHOW INTERFACE" on page 221.

Displaying Port Configuration

To display the current port configuration settings, use the SHOW RUNNING-CONFIG INTERFACE command in the Privileged Exec mode. Here is the format:

show running-config interface *interface-list*

This example displays the settings for ports 1 and 2:

awplus# show running-config interface port1.0.7

See Figure 47 for an example of the display.

```
Interface port1.0.7
    switchport
    switchport mode access
    switchport access vlan 2
```

Figure 47. SHOW RUNNING-CONFIG INTERFACE Command

For a description of the command, see "SHOW RUNNING-CONFIG INTERFACE" on page 232.

188

Displaying or Clearing Port Statistics

To view packet statistics for the individual ports, use the SHOW PLATFORM TABLE PORT COUNTERS command in the Privileged Exec mode. Here is the format of the command:

```
show platform table port [port] counters
```

This example displays the statistics for ports 23 and 24:

```
awplus# show platform table port port1.0.23,port1.0.24
counter
```

The statistics are described in Table 16 on page 229.

To clear the port counters, use the CLEAR PORT COUNTER command, which has this format:

```
clear port counter port
```

This example clears the counters for ports 1 and 4:

```
awplus# clear port counter port1.0.1,port1.0.4
```

Displaying SFP Information

To view information on a plugged SFP on the switch, use the SHOW SYSTEM PLUGGABLE command in the Privileged Exec mode. Here is the format of the command:

```
show system pluggable
```

For more information about this command, see "SHOW SYSTEM PLUGGABLE" on page 235.

To view more detail information on a plugged SFP, use the following command:

```
awplus# show system pluggable detail
```

The fields are described in Table 16 on page 229.

Chapter 10
Port Parameter Commands

The port parameter commands are summarized in Table 11.

Table 11. Port Parameter Commands

Command	Mode	Description
"BACKPRESSURE" on page 194	Port Interface	Enables or disables backpressure on ports that are operating in half-duplex mode.
"BPLIMIT" on page 196	Port Interface	Specifies threshold levels for backpressure on ports.
"CLEAR PORT COUNTER" on page 197	User Exec and Privileged Exec	Clears the packet counters.
"DESCRIPTION" on page 198	Port Interface	Adds port descriptions.
"DUPLEX" on page 200	Port Interface	Configures the duplex modes.
"EGRESS-RATE-LIMIT" on page 202	Port Interface	Sets a limit on the amount of traffic that can be transmitted per second from the port.
"FCTRLLIMIT" on page 203	Port Interface	Specifies threshold levels for flow control.
"FLOWCONTROL" on page 204	Port Interface	Enables or disables flow control on ports that are operating in full-duplex mode.
"HOLBPLIMIT" on page 207	Port Interface	Specifies a threshold for head of line blocking events.
"NO EGRESS-RATE-LIMIT" on page 209	Port Interface	Disables egress rate limiting on the ports.
"NO FLOWCONTROL" on page 210	Port Interface	Disables flow control on ports.
"NO SHUTDOWN" on page 211	Port Interface	Activates disabled ports so that they resume forwarding network traffic again.
"NO SNMP TRAP LINK-STATUS" on page 212	Port Interface	Deactivates link traps.

Table 11. Port Parameter Commands (Continued)

Command	Mode	Description
"NO STORM-CONTROL" on page 213	Port Interface	Removes threshold limits for broadcast, multicast, or unknown unicast packets.
"POLARITY" on page 214	Port Interface	Sets the MDI/MDI-X settings on twisted pair ports.
"PURGE" on page 216	Port Interface	Restores the default settings.
"RENEGOTIATE" on page 217	Port Interface	Prompts ports that are using Auto-Negotiation to renegotiate their settings with the network devices.
"RESET" on page 218	Port Interface	Performs software resets on the ports.
"SHOW FLOWCONTROL INTERFACE" on page 219	Privileged Exec	Displays the current settings for flow control on the ports.
"SHOW INTERFACE" on page 221	Privileged Exec	Displays port settings.
"SHOW INTERFACE BRIEF" on page 225	Privileged Exec	Displays administrative and link statuses.
"SHOW INTERFACE STATUS" on page 227	Privileged Exec	Displays the speed and duplex mode settings of the ports.
"SHOW PLATFORM TABLE PORT COUNTERS" on page 229	Privileged Exec	Displays packet statistics for the individual ports.
"SHOW RUNNING-CONFIG INTERFACE" on page 232	Privileged Exec	Displays the settings of the specified ports.
"SHOW STORM-CONTROL" on page 233	Privileged Exec	Displays threshold settings for broadcast, multicast, and unknown unicast packets.
"SHOW SYSTEM PLUGGABLE" on page 235	Privileged Exec	Displays information about the SFP modules in the switch.
"SHOW SYSTEM PLUGGABLE DETAIL" on page 236	Privileged Exec	Displays information about the SFP modules in the switch.
"SHUTDOWN" on page 237	Port Interface	Disables ports to stop them from forwarding network traffic.
"SNMP TRAP LINK-STATUS" on page 238	Port Interface	Activates link traps.
"SPEED" on page 239	Port Interface	Manually sets port speed or activates Auto-Negotiation.

Table 11. Port Parameter Commands (Continued)

Command	Mode	Description
"STORM-CONTROL" on page 241	Port Interface	Sets a maximum limit of the number of broadcast, multicast, or unknown unicast packets forwarded by a port.

BACKPRESSURE

Syntax

```
backpressure on|off
```

Parameters

on

Activates backpressure on the ports.

off

Deactivates backpressure on the ports.

Mode

Port Interface mode

Description

Use this command to enable or disable backpressure on ports that are operating at 10 or 100 Mbps in half-duplex mode. Backpressure is used by ports during periods of packet congestion to temporarily stop their network counterparts from transmitting more packets. This prevents a buffer overrun and the subsequent loss and retransmission of network packets. A port initiates backpressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission.

To set backpressure on a port, you must configure the speed and duplex mode manually. You cannot set backpressure on a port that is using Auto-Negotiation.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example configures port 15 to 10 Mbps, half-duplex mode, and activates backpressure:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# speed 10
awplus(config-if)# duplex half
awplus(config-if)# backpressure on
```

194

This example configures ports 8 and 21 to 100 Mbps, half-duplex mode, with backpressure disabled:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8,port1.0.21
awplus(config-if)# speed 100
awplus(config-if)# duplex half
awplus(config-if)# backpressure off
```

BPLIMIT

Syntax

bplimit *bplimit*

Parameters

bplimit
> Specifies the number of cells for backpressure. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

Mode

Port Interface mode

Description

Use this command to specify a threshold level for backpressure on a port.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the threshold for backpressure on ports 15 and 20 to 7000 cells:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.20
awplus(config-if)# bplimit 7000
```

CLEAR PORT COUNTER

Syntax

```
clear port counter port
```

Parameters

port

Specifies the port whose packet counters you want to clear. You can specify more than one port at a time in the command.

Mode

User Exec mode and Privileged Exec mode

Description

Use this command to clear the packet counters of the ports. To display the counters, refer to "SHOW PLATFORM TABLE PORT COUNTERS" on page 229.

Example

This example clears the packet counters for ports 4 to 7:

```
awplus# clear port counter port1.0.4-port1.0.7
```

DESCRIPTION

Syntax

description *description*

Parameters

description
> Specifies a description of 1 to 240 alphanumeric characters for a port. Spaces and special characters are allowed.

Mode

Port Interface mode

Description

Use this command to add descriptions to the ports on the switch. The ports will be easier to identify if they have descriptions.

Use the NO form of this command to remove descriptions from ports without assigning new descriptions.

> **Note**
> The POWER-INLINE DESCRIPTION command is used to describe powered devices that are connected to the ports. For information about this command, see "POWER-INLINE DESCRIPTION" on page 267.

Confirmation Command

"SHOW INTERFACE" on page 221

Examples

This example assigns the description "printer22" to port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# description printer22
```

198

This example removes the current name from port 11 without assigning a new name:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11
awplus(config-if)# no description
```

DUPLEX

Syntax

```
duplex auto|half|full
```

Parameters

auto

> Activates Auto-Negotiation for the duplex mode, so that the duplex mode is set automatically.

half

> Specifies half-duplex mode.

full

> Specifies full-duplex mode.

Mode

Port Interface mode

Description

Use this command to set the duplex modes of the twisted pair ports. Ports operating in half-duplex mode can either receive packets or transmit packets, but not both at the same time, while ports operating in full-duplex can both send and receive packets, simultaneously.

> **Note**
> To avoid a duplex mode mismatch between switch ports and network devices, do not select Auto-Negotiation on ports that are connected to network devices on which the duplex modes are set manually. Switch ports that are set to Auto-Negotiation default to half duplex mode if they detect that the network devices are not using Auto-Negotiation. This may result in duplex mode mismatches in which the switch ports use half duplex mode and the network devices full duplex mode. To prevent this problem, always manually set the duplex mode on ports that are connected to network devices that are not using Auto-Negotiation.

Confirmation Command

"SHOW INTERFACE STATUS" on page 227

200

Examples

This example sets the duplex mode on port 11 half-duplex:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11
awplus(config-if)# duplex half
```

This example configures the duplex mode with Auto-Negotiation on port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# duplex auto
```

EGRESS-RATE-LIMIT

Syntax

```
egress-rate-limit value
```

Parameters

value

Specifies the maximum amount of traffic that can be transmitted from the port. The value is kilobits per second. The range is 64 to 1,000,000 kilobits per second.

Mode

Port Interface mode

Description

Use this command to set a limit on the amount of traffic that can be transmitted per second from the port.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the egress rate limit to 1,000,000 kilobits per second on ports 15, 16 and 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.16,port1.0.21
awplus(config-if)# egress-rate-limit 1000000
```

FCTRLLIMIT

Syntax

fctrllimit *fctrllimit*

Parameters

fctrllimit

Specifies the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

Mode

Port Interface mode

Description

Use this command to specify threshold levels for flow control on the ports.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the threshold level for flow control on port 14 to 5000 cells:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# fctrllimit 5000
```

FLOWCONTROL

Syntax

```
flowcontrol send|receive|both on|off
```

Parameter

send

Controls whether a port sends pause packets during periods of packet congestion, to initiate flow control.

receive

Controls whether a port, when it receives pause packets from its network counterpart, stops sending packets.

on

Activates flow control.

off

Deactivates flow control.

Mode

Port Interface mode

Description

Use this command to enable or disable flow control on ports that are operating in full-duplex mode. Ports use flow control when they are experiencing traffic congestion and need to temporary stop their link partners from transmitting any more traffic. This allows them time to process the packets already in their buffers.

A port that is experiencing traffic congestion initiates flow control by sending pause packets. These packets instruct the link partner to stop transmitting packets. A port continues to issue pause packets so long as the traffic congestion persists. Once the condition has cleared, a port stops sending pause packets to allow its link partner to resume the transmission of packets.

The ports on the switch can both send pause packets during periods of traffic congestion and stop transmitting packets when they receive pause packets from their link partners. You can control both aspects of flow control separately on the ports.

The RECEIVE parameter in the command controls the behavior of a port when it receives pause packets from a network device. If receive is on, a port stops sending packets in response to pause packets from its link

204

partner. If it is off, a port does not respond to pause packets and continues to transmit packets. At the default setting, the receive portion of flow control is off.

The SEND parameter determines whether a port sends pause packets when it experiences traffic congestion. If send is on, a port sends pause packets to signal its link partner of the condition and to stop the transmission of more packets. If send is off, a port does not send pause packets during periods of traffic congestion. At the default setting, the send portion of flow control is off.

To configure flow control on a port, you must disable Auto-Negotiation and set the speed and duplex mode manually. A port set to Auto-Negotiation always uses flow control when operating in full-duplex mode.

Confirmation Command

Examples

This example configures port 19 to 100 Mbps, full-duplex mode, with both the send and receive parts of flow control enabled:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.19
awplus(config-if)# speed 100
awplus(config-if)# duplex full
awplus(config-if)# flowcontrol send on
awplus(config-if)# flowcontrol receive on
```

This example configures ports 18 to 21 and 24 to 10 Mbps, full-duplex mode, with both the send and receive portions of flow control disabled. The ports will neither respond to pause packets from their link partners by ceasing transmission nor will they issue pause packets during periods of traffic congestion:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18-port1.0.21,port1.0.24
awplus(config-if)# speed 10
awplus(config-if)# duplex full
awplus(config-if)# flowcontrol receive off
awplus(config-if)# flowcontrol send off
```

This example configures port 1 and 2 to 10 Mbps, full-duplex mode. The send portion of flow control is disabled so that the ports do not send pause packets during periods of traffic congestion. But the receive portion is enabled so that the ports respond to pause packets from their network counterparts by temporarily ceasing transmission:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# speed 10
awplus(config-if)# duplex full
awplus(config-if)# flowcontrol send off
awplus(config-if)# flowcontrol receive on
```

HOLBPLIMIT

Syntax

holbplimit *holbplimit*

Parameter

holbplimit
> Specifies the threshold at which a port signals a head of line blocking event. The threshold is specified in cells. A cell is 128 bytes. The range is 1 to 8,191 cells; the default is 7,168 cells.

Mode

Port Interface mode

Description

Use this command to specify a threshold for head of line blocking events on the ports. Head of line (HOL) blocking is a problem that occurs when a port on the switch becomes oversubscribed because it is receiving more packets from other switch ports than it can transmit in a timely manner.

An oversubscribed port can prevent other ports from forwarding packets to each other because ingress packets on a port are buffered in a First In, First Out (FIFO) manner. If a port has, at the head of its ingress queue, a packet destined for an oversubscribed port, it will not be able to forward any of its other packets to the egress queues of the other ports.

A simplified version of the problem is illustrated in Figure 48 on page 208. It shows four ports on the switch. Port D is receiving packets from two ports— 50% of the egress traffic from port A and 100% of the egress traffic from port B. Not only is port A unable to forward packets to port D because port D's ingress queues are filled with packets from port B, but port A is also unable to forward traffic to port C because its egress queue has frames destined to port D that it is unable to forward.
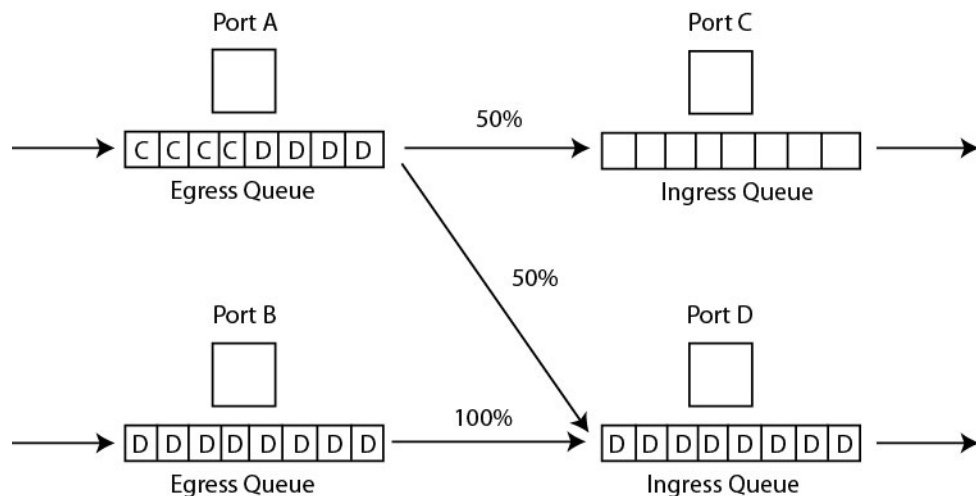
Figure 48. Head of Line Blocking

The HOL Limit parameter can help prevent this problem from occurring. It sets a threshold on the utilization of a port's egress queue. When the threshold for a port is exceeded, the switch signals other ports to discard packets to the oversubscribed port.

For example, referring to the figure above, when the utilization of the storage capacity of port D exceeds the threshold, the switch signals the other ports to discard packets destined for port D. Port A drops the D packets, enabling it to once again forward packets to port C.

The number you enter for this value represents cells. A cell is 128 bytes. The range is 1 to 8,191 cells; the default is 7,168 cells.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the head of line blocking threshold on port 9 to 5,000 cells:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.9
awplus(config-if)# holbplimit 5000
```

208

NO EGRESS-RATE-LIMIT

Syntax

```
no egress-rate-limit
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable egress rate limiting on the ports.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example disable egress rate limiting on the ports 4 and 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.5
awplus(config-if)# no egress-rate-limit
```

NO FLOWCONTROL

Syntax

```
no flowcontrol
```

Parameter

None

Mode

Port Interface mode

Description

Use this command to disable flow control on ports.

Confirmation Command

"SHOW FLOWCONTROL INTERFACE" on page 219

Example

This example disables flow control on port 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# no flowcontrol
```

NO SHUTDOWN

Syntax

no shutdown

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable ports so that they forward packets again. This is the default setting for a port.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example enables port 22:

awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22
awplus(config-if)# no shutdown

NO SNMP TRAP LINK-STATUS

Syntax

```
no snmp trap link-status
```

Parameter

None

Mode

Port Interface mode

Description

Use this command to deactivate SNMP link traps on the ports of the switch. The switch does not send traps when a port on which link trap is disabled experiences a change in its link state (i.e., goes up or down).

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example deactivates link traps on ports 18 and 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.23
awplus(config-if)# no snmp trap link-status
```

NO STORM-CONTROL

Syntax

```
no storm-control broadcast|multicast|dlf
```

Parameters

broadcast
> Specifies broadcast packets.

multicast
> Specifies multicast packets.

dlf
> Specifies unknown unicast packets.

Description

Use this command to remove packet threshold levels that were set on the ports with "STORM-CONTROL" on page 241.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example removes the threshold limit for broadcast packets on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no storm-control broadcast
```

This example removes the threshold limit for unknown unicast rate on port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no storm-control dlf
```

This example removes the threshold limit for multicast packets on port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no storm-control multicast
```

POLARITY

Syntax

```
polarity auto|mdi|mdix
```

Parameters

auto

 Activates auto-MDI/MDIX.

mdi

 Sets a port's wiring configuration to MDI.

mdix

 Sets a port's wiring configuration to MDI-X.

Mode

Port Interface mode

Description

Use this command to set the wiring configuration of twisted pair ports that are operating at 10 or 100 Mbps, in half- or full-duplex mode.

A twisted pair port that is operating at 10 or 100 Mbps can have one of two wiring configurations, known as MDI (medium dependent interface) and MDI-X (medium dependent interface crossover). To forward traffic, a port on the switch and a port on a network device must have different settings. For instance, the wiring configuration of a switch port has to be MDI if the wiring configuration on a port on a network device is MDIX.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example sets port 28 to the MDI wiring configuration:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.28
awplus(config-if)# polarity mdi
```

214

This example sets ports 4 and 18 to the MDI-X wiring configuration:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.18
awplus(config-if)# polarity mdix
```

This example activates auto-MDI/MDIX on ports 1 to 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.3
awplus(config-if)# polarity auto
```

PURGE

Syntax

```
purge
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to restore the default settings to these port parameters:

- ❐ Enabled status (NO SHUTDOWN)
- ❐ Description
- ❐ Speed
- ❐ Duplex mode
- ❐ MDI/MDI-X
- ❐ Flow control
- ❐ Backpressure
- ❐ Head of line blocking threshold
- ❐ Backpressure cells

Example

This example restores the default settings to ports 5, 6 and 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.6,port1.0.12
awplus(config-if)# purge
```

RENEGOTIATE

Syntax

```
renegotiate
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to prompt a port that is set to Auto-Negotiation to renegotiate its speed and duplex mode with its network device. You might use this command if you believe that a port and a network device did not establish the highest possible common settings during the Auto-Negotiation process.

Example

This example prompts port 18 to renegotiate its settings with its network counterpart:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18
awplus(config-if)# renegotiate
```

RESET

Syntax

```
reset
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to perform a hardware reset on the ports. The ports retain their parameter settings. The reset takes only a second or two to complete. You might reset a port if it is experiencing a problem.

Example

This example resets port 14:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# reset
```

218

SHOW FLOWCONTROL INTERFACE

Syntax

show flowcontrol interface *port*

Parameter

port
> Specifies the port whose flow control setting you want to view. You can specify just one port at a time.

Modes

Privileged Exec mode

Description

Use this command to display the current settings for flow control on the ports. An example of the information is shown in Figure 49.

```
PortSendReceive   RxPause     TxPause
   adminadmin
-------------------------   -------
1.0.13yesyes      6520        7823
```

Figure 49. SHOW FLOWCONTROL INTERFACE Command

The fields are described in Table 12.

Table 12. SHOW FLOWCONTROL INTERFACE Command

Parameter	Description
Port	Port number.
Send admin	Whether or not flow control is active on the transmit side of the port. If yes, the port transmits pause packets during periods of packet congestion. If no, the port does not transmit pause packets.
Receive admin	Whether or not flow control is active on the receive side of the port. If yes, the port stops transmitting packets when it receives pause packets from the other network device. If no, the port does not stop transmitting packets.

219

Table 12. SHOW FLOWCONTROL INTERFACE Command (Continued)

Parameter	Description
RxPause	The number of received pause packets.
TxPause	The number of transmitted pause packets.

Example

This command displays the flow control settings for port 2:

```
awplus# show flowcontrol interface port1.0.2
```

SHOW INTERFACE

Syntax

```
show interface [port]
```

Parameter

port

Specifies the port whose current status you want to view. You can display more than one port at a time. To display all the ports, do not include this parameter.

Modes

Privileged Exec mode

Description

Use this command to display the current operating status of the ports. An example of the information is shown in Figure 50 on page 222.

```
Interface port1.0.1

    Link is UP, administrative state is UP
    Address is 0015.77cc.e243

    Description:
    index 1 mtu 9198

    Unknown Ingress Multicast Blocking: Disabled

    Unknown Egress Multicast Blocking: Disabled

    SNMP link-status traps: Enabled (Suppressed in 0 sec.)

    Bandwidth 1g

    input packets 0, bytes 0, dropped 0, multicast packets 0

    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
Interface port1.0.2

    Link is UP, administrative state is UP

    Address is 0015.77cc.e244

    Description:
    index 1 mtu 9198

    Unknown Ingress Multicast Blocking: Disabled

    Unknown Egress Multicast Blocking: Disabled

    SNMP link-status traps: Enabled (Suppressed in 0 sec.)

    Bandwidth 1g

    input packets 0, bytes 0, dropped 0, multicast packets 0

    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
```

Figure 50. SHOW INTERFACE Command

The fields are described in Table 13.

Table 13. SHOW INTERFACE Command

Parameter	Description
Interface	Port number.

Table 13. SHOW INTERFACE Command (Continued)

Parameter	Description
Link is	The status of the link on the port. This field is UP when the port has a link with a network device, and DOWN when the port does not have a link.
Administrative state	The administrative state of the port. The administrative state will be DOWN if the port was disabled with the SHUTDOWN command. Otherwise, the administrative state of the port will be UP. To disable and enable ports, refer to "SHUTDOWN" on page 237 and "NO SHUTDOWN" on page 211, respectively.
Address is	The MAC address of the port.
Description	The port's description. To set the description, refer to "DESCRIPTION" on page 198.
Index mtu	The maximum packet size of the ports. The ports have a maximum packet size of 9198 bytes. This is not adjustable.
Unknown Ingress/Egress Multicast Blocking	The status of multicast blocking on the port. To set multicast blocking, refer to Chapter 25, "Multicast Commands" on page 447.
SNMP link-status traps	The status of SNMP link traps on the port. The switch sends link traps if the status is Enabled and does not send link traps if the status is Disabled. To enable and disable link traps, refer to "SNMP TRAP LINK-STATUS" on page 238 and "NO SNMP TRAP LINK-STATUS" on page 212, respectively.
Bandwidth	The current operating speed of the port. The bandwidth will be Unknown if the port does not have a link to a network device.
Input statistics	Ingress packet statistics.
Output statistics	Egress packet statistics.

Examples

This command displays the current operational state of all the ports:

```
awplus# show interface
```

This command displays the current operational state of ports 1 to 4:

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

SHOW INTERFACE BRIEF

Syntax

```
show interface brief
```

Parameter

None

Modes

Privileged Exec mode

Description

Use this command to display the administrative and link statuses of all of the ports on the switch. An example of the information is shown in Figure 51.

```
Interface StatusProtocol
 port1.0.1admin up down
 port1.0.2admin up down
 port1.0.3admin up down
 port1.0.4admin up down
 port1.0.5admin up down
 port1.0.6admin up down
```

Figure 51. SHOW INTERFACE BRIEF Command

The fields are described in Table 14.

Table 14. SHOW INTERFACE BRIEF Command

Field	Description
Interface	Indicates the port number.
Status	Indicates the administrative state of the port. The administrative state is DOWN if the port was disabled with the SHUTDOWN command. Otherwise, the administrative state of the port is UP. To disable and enable ports, refer to "SHUTDOWN" on page 237 and "NO SHUTDOWN" on page 211, respectively.

Table 14. SHOW INTERFACE BRIEF Command (Continued)

Field	Description
Protocol	Indicates the status of the link on the port. This field is UP when the port has a link with a network device, and DOWN when the port does not have a link.

Example

The following example displays the administrative and link statuses of all of the ports on the switch:

```
awplus# show interface brief
```

SHOW INTERFACE STATUS

Syntax

```
show interface [port] status
```

Parameter

port

Specifies the port whose parameter settings you want to view. You can display more than one port at a time. To display all the ports, do not include a port number.

Modes

Privileged Exec mode

Description

Use this command to display the speed, duplex mode, and VLAN settings of the ports. An example of the information is shown in Figure 52.

```
PortNameStatus    Vlan        Duplex        SpeedType
port1.0.1Port_01down3         half          10010/100/1000Base-T
port1.0.2Port_02up11          auto          auto10/100/1000Base-T
port1.0.2Port_02up2           auto          auto10/100/1000Base-T
port1.0.2Port_02up2           full          10010/100/1000Base-T
port1.0.2Port_02up2           auto          auto10/100/1000Base-T
```

Figure 52. SHOW INTERFACE STATUS Command

The fields are described in Table 15.

Table 15. SHOW INTERFACE STATUS Command

Parameter	Description
Port	Port number.
Name	Description of port. To set the description, refer to "DESCRIPTION" on page 198.
Status	Link status of the port. The status is Up if the port has a link to a network device. The status is Down if the port does not have a link.
VLAN	The ID of the VLAN in which the port is an untagged member.

227

Table 15. SHOW INTERFACE STATUS Command (Continued)

Parameter	Description
Duplex	The duplex mode setting of the port. The setting can be half, full or auto for Auto-Negotiation. To set the duplex mode, refer to "DUPLEX" on page 200.
Speed	The speed of the port. The settings are 10, 100, or 1000 Mbps, or auto for Auto-Negotiation.
Type	The Ethernet standard of the port.

Examples

This command displays the settings of all the ports:

```
awplus# show interface status
```

This command displays the settings of ports 17 and 18:

```
awplus# show interface port1.0.17-port1.0.18 status
```

SHOW PLATFORM TABLE PORT COUNTERS

Syntax

```
show platform table port [port] counters
```

Parameter

port

Specifies the port whose statistics you want to view. You can specify more than one port at a time in the command. To view all the ports, omit this parameter.

Modes

Privileged Exec mode

Description

Use this command to display the packet statistics for the individual ports on the switch. The statistics are described in Table 16. To clear the packet counters, refer to "CLEAR PORT COUNTER" on page 197.

Table 16. SHOW PLATFORM TABLE PORT COUNTERS Command

Parameter	Description
64 65-127 128-255 256-511 512-1023 1024-1518 1519-1522	Number of frames transmitted by the port, grouped by size.
General Counters	
Octets	Number of received and transmitted octets.
Pkts	Number received and transmitted packets.
CRCErrors	Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received by the port.
FCSErrors	Number of ingress frames that had frame check sequence (FCS) errors.

Table 16. SHOW PLATFORM TABLE PORT COUNTERS Command

Parameter	Description
MulticastPkts	Number of received and transmitted multicast packets.
BroadcastPkts	Number of received and transmitted broadcast packets
PauseMACCtrlFrms	Number of received and transmitted flow control pause packets.
OversizePkts	Number of received packets that exceeded the maximum size as specified by IEEE 802.3 (1518 bytes including the CRC).
Fragments	Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors).
Jabbers	Number of occurrences of corrupted data or useless signals the port has encountered.
UnsupportOpcode	Number of MAC Control frames with unsupported opcode.
UndersizePkts	Number of frames that were less than the minimum length as specified in the IEEE 802.3 standard (64 bytes including the CRC).
SingleCollsnFrm	Number of frames that were transmitted after at least one collision.
MultCollsnFrm	Number of frames that were transmitted after more than one collision.
LateCollisions	Number of late collisions.
ExcessivCollsns	Number of excessive collisions.
Collisions	Total number of collisions on the port.
Layer 3 Counters	
ifInUcastPkts	Number of ingress unicast packets.
ifOutUcastPkts	Number of egress unicast packets.
ifInDiscards	Number of ingress packets that were discarded.

Table 16. SHOW PLATFORM TABLE PORT COUNTERS Command

Parameter	Description
ifOutErrors	Number of packets that were discarded prior to transmission because of an error.
ipInHdrErrors	Number of ingress packets that were discarded because of a hardware error.
Miscellaneous Counters	
MAC TxErr	Number of frames not transmitted correctly or dropped due to an internal MAC transmit error.
MAC RxErr	Number of Receive Error events seen by the receive side of the MAC.
Drop Events	Number of frames successfully received and buffered by the port, but discarded and not forwarded.

Examples

This command displays the statistics for ports 21 and 23:

```
awplus# show platform table port port1.0.21,port1.0.23
counters
```

This command displays the statistics for all the ports on the switch:

```
awplus# show platform table port counters
```

SHOW RUNNING-CONFIG INTERFACE

Syntax

```
show running-config interface port
```

Parameters

port

Specifies a port, multiple ports, or a range of ports. For a detailed explanation on how to specify ports, see "Port Numbers in Commands" on page 58.

Modes

Privileged Exec mode

Description

Use this command to display the configuration settings of the ports. The command displays only the settings that have been changed from their default values and includes those values that have not yet been saved in the active boot configuration file. An example of the information is shown in Figure 53.

```
interface port1.0.1
    dot1x port-control auto
    no auth dynamic-vlan-creation

interface port1.0.3-port1.0.4
    switchport access vlan 2
```

Figure 53. SHOW RUNNING-CONFIG INTERFACE Command

Example

This example displays the configuration settings for ports 1, 3, and 4:

```
awplus# show running-config interface port1.0.1,port1.0.3-
port1.0.4
```

232

SHOW STORM-CONTROL

Syntax

show storm-control [*port*]

Parameters

port

> Specifies the port whose storm-control, threshold limit settings you want to view. You can specify more than one port at a time. To display all the ports, do not include this parameter.

Mode

Privileged Exec mode

Description

Use this command to display information about the threshold limit settings on the ports. Figure 54 shows an example of the information when you enter the following command:

awplus# show storm-control port1.0.15

```
Port     BcastLevel   Mcastlevel   Dlflevel
Port1.0.15 30100  100
```

Figure 54. SHOW STORM-CONTROL Command

See Table 17 for a description of the table headings.

Table 17. SHOW STORM-CONTROL Command

Column	Description
Port	Indicates the port number.
BcastLevel	Indicates the maximum number of ingress broadcast packets per second for the port. Broadcast packets beyond this number are discarded.
McastLevel	Indicates the maximum number of ingress multicast packets per second for the port. Multicast packets beyond this number are discarded.

Table 17. SHOW STORM-CONTROL Command (Continued)

Column	Description
DlfLevel	Indicates the maximum number of unknown unicast packets, destination lookup failure (DLF) packets per second for the port. DLF packets beyond this number are discarded.

Examples

This command displays the settings of all the ports:

```
awplus# show storm-control
```

This command displays the settings of ports 15 and 18:

```
awplus# show storm-control port1.0.15,port1.0.18
```

SHOW SYSTEM PLUGGABLE

Syntax

show system pluggable

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display information about the SFP modules in the switch.

```
 System Pluggable Information

PortVendorDevice  Serial NumberDatecode     Type
-----------------------------------------------------------
1.0.49ATIAT-SPSX  A03240R08420074120081018   1000BASE-SX
1.0.51ATIAT-SPSX  A03240R08420074920081018   1000BASE-SX
-----------------------------------------------------------
```

Figure 55. SHOW SYSTEM PLUGGABLE Command

Example

This example displays SFP module information:

awplus# show system pluggable

235

SHOW SYSTEM PLUGGABLE DETAIL

Syntax

show system pluggable detail

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display information about the SFP modules in the switch. See Figure 56. The SHOW SYSTEM PLUGGABLE DETAIL command provides more detailed information than the SHOW SYSTEM PLUGGABLE command. See "SHOW SYSTEM PLUGGABLE" on page 235.

```
Port1.0.49
==========
Vendor Name:ATI
Device Name:AT-SPSX
Device Type:1000BASE-SX
Serial Number:A03240R084200741
Manufacturing Datecode:20081018
SFP Laser Wavelength:850nm

Link Length Supported
   OM1 (62.5um) Fiber:270m
   OM2 (50um) Fiber:550m
```

Figure 56. SHOW SYSTEM PLUGGABLE DETAIL Command

The OM1 field specifies the link length supported by the pluggable transceiver using 62.5 micron multi-mode fiber. The OM2 field specifies the link length supported by the pluggable transceiver using 50 micron multi-mode fiber.

Example

This example displays detailed information about SFP modules:

awplus# show system pluggable detail

236

SHUTDOWN

Syntax

`shutdown`

Parameter

None

Mode

Port Interface mode

Description

Use this command to disable ports. Ports that are disabled do not forward traffic. You might disable ports that are unused to secure them from unauthorized use or that are having problems with network cables or their link partners. The default setting for the ports is enabled.

To reactivate a port, refer to "NO SHUTDOWN" on page 211.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example disables ports 15 and 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.16
awplus(config-if)# shutdown
```

SNMP TRAP LINK-STATUS

Syntax

```
snmp trap link-status
```

Parameter

None

Mode

Port Interface mode

Description

Use this command to activate SNMP link traps on the ports. The switch sends an SNMP trap to an SNMP trap receiver on your network whenever a port experiences a change in its link state.

To disable link traps on a port, refer to "NO SNMP TRAP LINK-STATUS" on page 212.

> **Note**
> For the switch to send SNMP traps, you must activate SNMP and specify one or more trap receivers. For instructions, refer to Chapter 63, "SNMPv1 and SNMPv2c Commands" on page 975 or Chapter 64, "SNMPv3 Commands" on page 999.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example activates link traps on port 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22
awplus(config-if)# snmp trap link-status
```

238

SPEED

Syntax

```
speed auto|10|100|1000
```

Parameters

auto

Activates Auto-Negotiation so that the speed is configured automatically.

10

Specifies 10 Mbps.

100

Specifies 100 Mbps.

1000

Specifies 1000 Mbps. This setting should not be used on twisted pair ports. For 1000Mbps, full duplex operation, a twisted pair port must be set to Auto-Negotiation.

Mode

Port Interface mode

Description

Use this command to manually set the speeds of the twisted pair ports or to activate Auto-Negotiation.

Confirmation Commands

❒ Configured speed: "SHOW INTERFACE STATUS" on page 227

❒ Current operating speed: "SHOW INTERFACE" on page 221

Examples

This example sets the speed on ports 11 and 17 to 100 Mbps:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11,port1.0.17
awplus(config-if)# speed 100
```

This example activates Auto-Negotiation on port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# speed auto
```

240

STORM-CONTROL

Syntax

```
storm-control broadcast|multicast|dlf level value
```

Parameters

broadcast
> Specifies broadcast packets.

multicast
> Specifies multicast packets.

dlf
> Specifies unknown unicast packets.

level
> Specifies the maximum number of ingress packets per second of the designated type the port will forward. The range is 0 to 33,554,431 packets.

Mode

Port Interface mode

Description

Use this command to set maximum thresholds for the ingress packets on the ports. Ingress packets that exceed the thresholds are discarded by the ports. Thresholds can be set independently for broadcast packets, multicast packets, and unknown unicast packets. To view the current thresholds of the ports, refer to "SHOW RUNNING-CONFIG" on page 158.

To remove threshold levels from the ports, refer to "NO STORM-CONTROL" on page 213.

Confirmation Commands

"SHOW STORM-CONTROL" on page 233

"SHOW RUNNING-CONFIG" on page 158

Examples

This example sets the maximum threshold level of 5,000 packets per second for ingress broadcast packets on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# storm-control broadcast level 5000
```

This example sets the maximum threshold level of 100,000 packets per second for ingress multicast packets on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# storm-control multicast level 100000
```

This example sets the threshold level of 200,000 packets per second for ingress unknown unicast packets on ports 15 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.17
awplus(config-if)# storm-control dlf level 200000
```

Chapter 11
Power Over Ethernet

Overview

The AT-9000/12PoE and AT-9000/28PoE switches feature Power over Ethernet (PoE) on the 10/100Base-Tx ports. PoE is used to supply power to network devices over the same twisted pair cables that carry the network traffic.

The main advantage of PoE is that it can make it easier to install a network. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE-compatible devices wherever they are needed without having to worry about whether there is a power source nearby.

Power Sourcing Equipment (PSE)

A device that provides PoE to other network devices is referred to as power sourcing equipment (PSE). The AT-9000/12PoE and AT-9000/28PoE switches are PSE devices providing DC power to the network cable and functioning as a central power source for other network devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

PD Classes

PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The AT-9000 PoE switches support all five classes listed in Table 18.

Table 18. IEEE Powered Device Classes

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	30W	12.95W to 25.5W

Power Budget

Power budget is the maximum amount of power that the PoE switch can provide at one time to the connected PDs.

The AT-9000/12POE switch has a power budget of 125 watts. The AT-9000/28POE switch has a power budget of 370 watts. These are the maximum amounts of power the switches can provide at one time to the powered devices.

The AT-9000/28POE switch has two power supplies. Each power supply is responsible for providing 185 watts, or half, of the power budget. Both power supplies must be connected to AC power sources for the switch to provide the full 370 watts. The power budget is reduced to 185 watts if only one power supply is connected to a power source.

Port Prioritization

As long as the total power requirements of the PDs is less than the total available power of the switch, it can supply power to all of the PDs. However, when the PD power requirements exceed the total available power, the switch denies power to some ports based on a process called port prioritization.

The ports on the PoE switch are assigned to one of three priority levels. These levels and descriptions are listed in Table 19.

Table 19. PoE Port Priorities

Priority Level	Description
Critical	This is the highest priority level. Ports set to the Critical level are guaranteed to receive power before any of the ports assigned to the other priority levels.
High	Ports set to the High level receive power only when all the ports assigned to the Critical level are already receiving power.
Low	This is the lowest priority level. Ports set to the Low level receive power only when all the ports assigned to the Critical and High levels are already receiving power. This level is the default setting.

Without enough power to support all the ports set to the same priority level at one time, the switch provides power to the ports based on the port number, in ascending order. For example, when all of the ports in the switch are set to the low priority level, and the power requirements are exceeded on the switch, port 1 has the highest priority level, port 2 has the next highest priority level and so forth.

Enabling and Disabling PoE

Enabling PoE on ports allows the switch to supply power to PDs connected to the ports. In order for PDs to receive power, PoE must be enabled on the ports. By default, PoE is enabled on all the ports on the PoE switch.

The switch detects whether or not a network device connected to the port is a valid PD. If the device is not a valid PD, the port functions as a regular Ethernet port even when PoE is enabled on the port. The PoE feature remains activated on the port, but no power is delivered to the device.

Disabling PoE on the port turns off the power supply to the port. You may want to disable PoE on the ports used only for data traffic in order to prevent them from unauthorized power use.

There are two ways to disable and enable PoE:

- ❐ Globally: all the ports on the switch at a time.
- ❐ Individually: on a port basis.

To enable PoE globally, use the SERVICE POWER-INLINE command in the Global Configuration mode. See "SERVICE POWER-INLINE" on page 273. The NO SERVICE POWER-INLINE command disables PoE on all the ports on the switch. See "NO SERVICE POWER-INLINE" on page 264.

To enable PoE on an individual port basis, use the POWER-INLINE ENABLE command in the Port Interface mode. See "POWER-INLINE ENABLE" on page 268. The NO POWER-INLINE command disables PoE on a port. See "NO POWER-INLINE ENABLE" on page 260.

This example enables PoE globally:

```
awplus> enable
awplus# configure terminal
awplus(config)# service power-inline
```

This example disables PoE globally:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service power-inline
```

This example enables PoE individually on port 6 and port 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6,port1.0.8
awplus(config-if)# power-inline enable
```

This example disables PoE individually on port 5 to port 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5-port1.0.8
awplus(config-if)# no power-inline enable
```

Adding PD Descriptions to Ports

PDs connected to the ports are easier to identify if you give them descriptions. To add descriptions to PDs, use the POWER-INLINE DESCRIPTION command in the Port Interface mode. Here is the format:

```
power-inline description description
```

The *description* parameter can consist of up to 256 alphanumeric characters. Spaces and special characters are allowed. You can assign a description to more than one port at a time. See "POWER-INLINE DESCRIPTION" on page 267.

To remove the current description from the port without assigning a new one, use the NO POWER-INLINE DESCRIPTION command. See "NO POWER-INLINE DESCRIPTION" on page 259.

This example adds a PD description of "Desk Phone" to port 1.0.5 and port1.0.6:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.6
awplus(config-if)# power-inline description Desk Phone
```

This example removes the description previously added to the port 6:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no power-inline description
```

> **Note**
> To add a general description to a port, use the DESCRIPTION command. For more information, see "DESCRIPTION" on page 198.

Prioritizing Ports

When the total power requirements of the PDs exceed the total available power of the switch, the switch denies power to one or more ports based on port prioritization.To guarantee power to the most critical PDs before any other PDs, the switch allows you to prioritize the ports for power supply.

You can assign one of three priority levels to a port: Critical, High, and Low. See "Port Prioritization" on page 245 for details. By default, all ports are set to the Low priority level. To change the priority level, use the POWER-INLINE PRIORITY command. Here is the format:

```
power-inline priority critical | high | low
```

To guarantee that the most critical PDs receive power, assign the highest priority level to the PDs. See "POWER-INLINE PRIORITY" on page 270.

To reset the priority level to the default Low level, use the NO POWER-INLINE PRIORITY command. See "NO POWER-INLINE PRIORITY" on page 262.

This example assigns ports 1, 2, and 3 to the Critical priority level to guarantee these ports receive power before any other ports with the High or Low priority level:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.3
awplus(config-if)# power-inline priority critical
```

This example assigns port 4 to port 10 to the High priority level so that the ports receive power before any ports with the Low priority level:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4-port1.0.10
awplus(config-if)# power-inline priority high
```

This example sets port 8 to the Low priority level:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# no power-inline priority
```

Managing the Maximum Power Limit on Ports

To manage the switch's power and optimize its power distribution, the switch allows you to adjust the power limit that the switch provides to each port. The switch automatically sets a default power limit to the port where a PD is connected and allows you to change the default settings.

The switch detects the power class of a PD when the PD is connected to the port. PDs are assigned one of five classes described in "PD Classes" on page 244. Each class has a maximum power. The switch sets this value as a default power limit to the port where the PD is connected.

For example, you connect an IP phone to port 1 on the PoE switch. The switch detects that the power class of the IP phone is 2. The maximum power output from the switch for a PD of class 2 is 7.0 watts. Thus, the switch sets 7.0 watts as the default power limit to port 1.

If a PD connected to the port does not support power classification, a default class of 0 is assigned to the PD. The maximum power for a PD of class 0 is 15.4 watts so that the switch sets 15.4 watts to the default power limit to the port.

To change a default power limit to the port, use the POWER-INLINE MAX command in the Port Interface mode. Specify the value in milliwatts (mW) See "POWER-INLINE MAX" on page 269.

This example changes the maximum power that the switch provides port 2 to 4.0 watts (4000 milliwatts):

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline max 4000
```

250

Managing Legacy PDs

The PoE switch automatically detects whether or not a device plugged into the PoE-enabled port is a valid PD. The switch supports PDs compliant with the IEEE 802.3af and IEEE 802.3at PoE standards. In addition, the switch supports legacy PDs that were designed before the IEEE standards were finalized.

If the switch detects the connected device as an invalid PD, the port functions as a regular Ethernet port. The PoE feature remains activated on the port, but no power is delivered to the PD.

To enable the switch to detect legacy PDs as valid PDs, use the POWER-INLINE ALLOW-LEGACY command to provide power to legacy PDs. See "POWER-INLINE ALLOW-LEGACY" on page 266. To disable the switch to detect legacy PDs as valid PDs, use the NO POWER-INLINE ALLOW-LEGACY command not to provide power to legacy PDs. By default, the switch detects legacy PDs as valid PDs. See "NO POWER-INLINE ALLOW-LEGACY" on page 258.

This example enables the switch to detect legacy PDs as valid PDs on port 1 to port 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.3
awplus(config-if)# power-inline allow-legacy
```

This example disables the switch to detect legacy PDs as valid PDs on ports 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no power-inline allow-legacy
```

Monitoring Power Consumption

You can monitor the power consumption of the switch and PDs by configuring the unit to transmit an SNMP power-inline trap if their combined power requirements exceed a defined threshold. The threshold is specified as a percentage of the switch's nominal power, which is the total available power of the switch. You can view the nominal power with "SHOW POWER-INLINE" on page 274. The threshold has the range of 1 to 99%. You may specify only one threshold. The commands for setting the threshold and activating the trap are listed in Table 20.

Table 20. Receiving Power Consumption Notification

To Do This Task	Use This Command
Set the power threshold as a percentage of the switch's nominal power.	POWER-INLINE USAGE-THRESHOLD
Activate SNMP on the switch.	SNMP-SERVER
Activate the transmission of SNMP trap for PoE.	SNMP-SERVER ENABLE TRAP POWER-INLINE

Note
You have to configure SNMP to use the trap. For instructions, refer to Chapter 62, "SNMPv1 and SNMPv2c" on page 963 or Chapter 64, "SNMPv3 Commands" on page 999.

This example configures the switch to send the SNMP power-inline trap if the power requirements of the switch and PDs exceed 90% of its nominal power:

```
awplus> enable
awplus# configure terminal
awplus(config)# power-inline usage-threshold 90
awplus(config)# snmp-server
awplus(config)# snmp-server enable trap power-inline
```

252

Displaying PoE Information

The switch allows you to display PoE information using three commands. Each command displays a different set of PoE information as described in Table 21.

Table 21. PoE Show Commands

Command	Description
SHOW POWER-INLINE	Displays PoE information about the switch and all the ports on the switch.
SHOW POWER-INLINE COUNTERS	Displays the PoE event counters for the ports.
SHOW POWER-INLINE INTERFACE	Displays PoE information of specified ports.
SHOW POWER-INLINE INTERFACE DETAIL	Displays detailed PoE information of the specified ports.

This example displays PoE information on both the switch and all the ports on the switch:

```
awplus# show power-inline
```

Figure 57 shows an example of the information the command displays. The columns are described in Table 23 on page 275.

```
PoE Status:
Nominal Power: 490W
Power Allocated: 346.0W
Actual Power Consumption: 151.0W
Operational Status: On
Power Usage Threshold: 80% (392W)
PoE Interface:

Interface   Admin     Pri    Oper       Power(mW) Device   Class  Max(mW)
port1.0.1  Enabled   Low   Powered  3840        Phone#1  1      4000 [C]
port1.0.2  Enabled   High  Powered  6720        n/a      2      7000 [C]
port1.0.3  Enabled   Low   Powered  14784       n/a      3      15400 [C]
port1.0.4  Enabled   Crit  Powered  14784       n/a      3      15400 [C]
port1.0.5  Enabled   Crit  Powered  3840        Phone#2  1      4000 [C]
port1.0.6  Enabled   High  Powered  6720        n/a      2      7000 [C]
port1.0.7EnabledLowPowered14784n/a315400 [C]
```

Figure 57. SHOW POWER-INLINE Command

This example displays the PoE information of port 1 through port 4:

```
awplus# show power inline interface port1.0.1-port1.0.4
```

Figure 58 shows an example of the information the command displays. The columns are described in Table 23 on page 275.

```
Interface   Admin      Pri    Oper      Power   Device        Class   Max(mW)
port1.0.1   Disabled   Low    Disabled  0       n/a           0       15400 [C]
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           0       15400 [C]
```

Figure 58. SHOW POWER-INLINE INTERFACE Command

This example displays the detailed PoE information of port 10:

```
awplus# show power inline interface port1.0.10 detail
```

Figure 59 shows an example of the information the command displays. The columns are described in Table 25 on page 280.

```
Interface port1.0.10
    Powered device type: Desk Phone #1
    PoE admin enabled
     Low Priority
    Detection status: Powered
    Current power consumption: 00 mW
    Powered device class: 1
    Power allocated: 5000 mW (from configuration)
    Detection of legacy device is disabled
    Powered pairs: Data
```

Figure 59. SHOW POWER-INLINE INTERFACE DETAIL Command

Chapter 12
Power Over Ethernet Commands

The Power over Ethernet (PoE) commands are summarized in Table 22. These commands are only supported on the PoE switches.

Table 22. Power over Ethernet Commands

Command	Mode	Description
"CLEAR POWER-INLINE COUNTERS INTERFACE" on page 257	Privileged Exec	Clears the PoE event counters on the ports.
"NO POWER-INLINE ALLOW-LEGACY" on page 258	Port Interface	Configures ports to deny power to legacy powered devices (PDs).
"NO POWER-INLINE DESCRIPTION" on page 259	Port Interface	Deletes the PD descriptions.
"NO POWER-INLINE ENABLE" on page 260	Port Interface	Disables PoE on the ports.
"NO POWER-INLINE MAX" on page 261	Port Interface	Restores a port's power limit to the default value.
"NO POWER-INLINE PRIORITY" on page 262	Port Interface	Restores a port's priority setting to the default Low level.
"NO POWER-INLINE USAGE-THRESHOLD" on page 263	Global Configuration	Resets the power usage threshold to the default 80%.
"NO SERVICE POWER-INLINE" on page 264	Global Configuration	Disables PoE on all of the ports on the switch.
"NO SNMP-SERVER ENABLE TRAP POWER-INLINE" on page 265	Global Configuration	Disables the SNMP power-inline trap.
"POWER-INLINE ALLOW-LEGACY" on page 266	Port Interface	Configures a port to support legacy PDs.
"POWER-INLINE DESCRIPTION" on page 267	Port Interface	Adds a PD description to a port.
"POWER-INLINE ENABLE" on page 268	Port Interface	Enables PoE on a port.
"POWER-INLINE MAX" on page 269	Port Interface	Specifies the power limit of a port.

Table 22. Power over Ethernet Commands (Continued)

Command	Mode	Description
"POWER-INLINE PRIORITY" on page 270	Port Interface	Assigns a PoE priority level to a port.
"POWER-INLINE USAGE-THRESHOLD" on page 272	Global Configuration	Sets the power threshold for the SNMP power-inline trap.
"SERVICE POWER-INLINE" on page 273	Global Configuration	Activates PoE on all of the ports on the switch.
"SHOW POWER-INLINE" on page 274	Privileged Exec	Displays switch and port PoE information.
"SHOW POWER-INLINE COUNTERS INTERFACE" on page 277	Privileged Exec	Displays the port PoE event counters.
"SHOW POWER-INLINE INTERFACE" on page 279	Privileged Exec	Displays port PoE information.
"SHOW POWER-INLINE INTERFACE DETAIL" on page 280	Privileged Exec	Displays additional port PoE information.
"SNMP-SERVER ENABLE TRAP POWER-INLINE" on page 283	Global Configuration	Activates the SNMP power-inline trap for PoE.

CLEAR POWER-INLINE COUNTERS INTERFACE

Syntax

```
clear power-inline counters interface [port]
```

Parameter

port
    Specifies a port. You can specify more than one port and clear event counters for multiple ports.

Mode

Privileged Exec mode

Description

Use this command to clear the PoE port event counters. To clear all of the port counters, do not enter a port number.

Confirmation Command

"SHOW POWER-INLINE COUNTERS INTERFACE" on page 277

Examples

This example clears all of the PoE port event counters:

```
awplus# clear power-inline counters interface
```

This example clears the event counters on ports 4 to 6:

```
awplus# clear power-inline counters interface port1.0.4-
port1.0.6
```

NO POWER-INLINE ALLOW-LEGACY

Syntax

```
no power-inline allow-legacy
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure the ports to deny power to legacy PDs. Legacy PDs are PoE devices that were designed before the IEEE 802.3af and IEEE 802.3at PoE standards were finalized. This is the default setting for the ports.

Confirmation Command

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example configures ports 1 to 12 to deny power to legacy PDs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.12
awplus(config-if)# no power-inline allow-legacy
```

NO POWER-INLINE DESCRIPTION

Syntax

```
no power-inline description
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to delete PD descriptions from the ports.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

The following example deletes the PD description from port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no power-inline description
```

NO POWER-INLINE ENABLE

Syntax

```
no power-inline enable
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable PoE on the ports. Ports do not transmit power when PoE is disabled, but they do forward network traffic.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

The following example disables PoE on ports 10, 11 and 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.10-port1.0.12
awplus(config-if)# no power-inline enable
```

NO POWER-INLINE MAX

Syntax

```
no power-inline max
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to restore the default maximum power limits on the ports. The default power limits are based on the power classes of the PDs. See "Managing the Maximum Power Limit on Ports" on page 250 for details.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example restores the default maximum power limit on port 6:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no power-inline max
```

NO POWER-INLINE PRIORITY

Syntax

```
no power-inline priority
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to restore the default Low priority setting to the ports.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example restores the default Low priority level to port 20:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20
awplus(config-if)# no power-inline priority
```

NO POWER-INLINE USAGE-THRESHOLD

Syntax

```
no power-inline usage-threshold
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to reset the power usage threshold to the default 80%. The switch sends an SNMP power-inline trap if the power requirements of the switch and PDs exceed the defined threshold.

Confirmation Command

"SHOW POWER-INLINE" on page 274

Example

This example restores the default power usage threshold of 80%:

```
awplus> enable
awplus# configure terminal
awplus(config)# no power-inline usage-threshold
```

NO SERVICE POWER-INLINE

Syntax

```
no service power-inline
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable PoE on the switch. The ports do not transmit power to the PDs when PoE is disabled, but they do forward network traffic. The default setting for PoE is enabled.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example disables PoE on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service power-inline
```

264

NO SNMP-SERVER ENABLE TRAP POWER-INLINE

Syntax

```
no snmp-server enable trap power-inline
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the transmission of SNMP power-inline traps. The switch sends this trap if the power requirements of the switch and PDs exceed the threshold set with "POWER-INLINE USAGE-THRESHOLD" on page 272

Confirmation Command

"SHOW RUNNING-CONFIG SNMP" on page 985

Example

The following example disables the SNMP power-inline trap:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server enable trap power-inline
```

POWER-INLINE ALLOW-LEGACY

Syntax

```
power-inline allow-legacy
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure the ports to support legacy PDs. Legacy PDs are PoE devices that were designed before the IEEE 802.3af and IEEE 802.3at PoE standards were finalized. The default setting is no support for legacy PDs.

Confirmation Commands

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example configures ports 1 to 6 to support legacy PDs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# power-inline allow-legacy
```

POWER-INLINE DESCRIPTION

Syntax

```
power-inline description description
```

Parameters

description
> Specifies a PD description of up to 256 alphanumeric characters. Spaces and special characters are allowed.

Mode

Port Interface mode

Description

Use this command to add PD descriptions to the ports to make the ports and PDs easier to identify.

> **Note**
> To add a general description to a port, use the DESCRIPTION command. For more information, see "DESCRIPTION" on page 198.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example adds the PD description "Surveillance Camera5" to port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# power-inline description Surveillance
Camera5
```

POWER-INLINE ENABLE

Syntax

```
power-inline enable
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable PoE on the ports. This is the default setting.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example enables PoE on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# power-inline enable
```

POWER-INLINE MAX

Syntax

```
power-inline max max_power
```

Parameters

max_power

Specifies the maximum power limit of the ports in milliwatts (mW).
The range is 4000 to 30000 mW.

Mode

Port Interface mode

Description

Use this command to set the maximum power limits on the ports. The
maximum power limit is the maximum amount of power a port may
transmit to a PD. Ports can have different limits. The default power limits
are based on the classes of the PDs. See "Managing the Maximum Power
Limit on Ports" on page 250 for details.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example sets the maximum power limits on ports 1 to port 6 to 6.5
watts:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# power-inline max 6500
```

POWER-INLINE PRIORITY

Syntax

```
power-inline priority critical|high|low
```

Parameters

critical

Sets ports to the Critical priority level for PoE ports. Ports set to the Critical level are guaranteed power before any of the ports assigned to the other priority levels.

high

Sets ports to the High priority level. Ports set to the High level receive power only when all of the ports assigned to the Critical level are already receiving power.

low

Sets ports to the Low priority level. Ports set to the Low level receive power only when all of the ports assigned to the critical and high levels are already receiving power. This level is the default setting.

Mode

Port Interface mode

Description

Use this command to assign PoE priority levels to the ports. The priority levels are Low, High, and Critical. Ports connected to the most critical PDs should be assigned the Critical level to guarantee them power before any of the other ports in the event the switch does not have enough power for all of the PDs.

If the switch does not have enough power to support all the ports set to the same priority level, it allocates power based on port number, in ascending order. For example, if all of the ports are set to the Low priority level, port 1 has the highest priority level, port 2 has the next highest priority level and so forth.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example assigns the Critical priority level to port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# power-inline priority critical
```

POWER-INLINE USAGE-THRESHOLD

Syntax

```
power-inline usage-threshold threshold
```

Parameters

threshold
>   Specifies the power usage threshold in a percentage of the switch's total available system and PoE power. The range is 1 to 99%.

Mode

Global Configuration mode

Description

Use this command to set a threshold of the switch's total available system and PoE power. An SNMP trap is transmitted if the requirements of the switch and the PDs exceed the threshold. To activate the trap, refer to "SNMP-SERVER ENABLE TRAP POWER-INLINE" on page 283. The default setting is 80%.

Confirmation Command

"SHOW POWER-INLINE" on page 274

Example

This example sets the threshold to 90% of the switch's total available power:

```
awplus> enable
awplus# configure terminal
awplus(config)# power-inline usage-threshold 90
```

SERVICE POWER-INLINE

Syntax

```
service power-inline
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable PoE on the switch. This is the default setting.

Confirmation Commands

"SHOW POWER-INLINE" on page 274

"SHOW POWER-INLINE INTERFACE" on page 279

"SHOW POWER-INLINE INTERFACE DETAIL" on page 280

Example

This example enables PoE on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# service power-inline
```

SHOW POWER-INLINE

Syntax

```
show power-inline
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display operational information about PoE. An example is shown in Figure 60. The fields are described in Table 23 on page 275.

```
PoE Status:
Nominal Power: 490W
Power Allocated: 346.0W
Actual Power Consumption: 151.0W
Operational Status: On
Power Usage Threshold: 80% (392W)
PoE Interface:

Interface  Admin    Pri   Oper      Power(mW) DeviceClassMax(mW)
port1.0.1  Enabled  Low   Powered   3840      n/a1     4000 [C]
port1.0.2  Enabled  High  Powered   6720      n/a2     7000 [C]
port1.0.3  Enabled  Low   Powered   14784     n/a3     15400 [C]
port1.0.4  Enabled  Crit  Powered   14784     n/a3     15400 [C]
port1.0.5  Enabled  Crit  Powered   3840      n/a1     4000 [C]
port1.0.6  Enabled  High  Powered   6720      n/a2     7000 [C]
port1.0.7EnabledLowPowered14784n/a315400 [C]
```

Figure 60. SHOW POWER-INLINE Command

Table 23. SHOW POWER-INLINE Command

Field	Description
Nominal Power	The switch's total available power in watts (W).
Power Allocated	The available power in watts (W) for PDs. This value is updated every 5 seconds.
Actual Power Consumption	The current power consumption in watts (W) of the PDs. This value is updated every 5 seconds.
Operational Status	The operational status of the power supply units (PSU) in the switch. The status can be one of the following: ❑ On: The units are powered on. ❑ Fault: One of the power supplies has encountered a problem.
Power Usage Threshold	The SNMP power-inline trap threshold. A SNMP trap is transmitted if the power requirements of the switch and PDs exceed the threshold. This parameter is set with "POWER-INLINE USAGE-THRESHOLD" on page 272.
PoE Interface	A table of port PoE information.
Interface	The port number.
Admin	The status of PoE on the port. The status can be one of the following: ❑ Enabled: PoE is enabled. The port can transmit power to a PD. PoE is enabled with "POWER-INLINE ENABLE" on page 268. ❑ Disabled: PoE is disabled. The port does not supply power to a PD, but it does forward network traffic. PoE is disabled with "NO POWER-INLINE ENABLE" on page 260.
Pri	The port's PoE priority level. This parameter is set with "POWER-INLINE PRIORITY" on page 270. The priority level can be one of the following: ❑ Low: The lowest priority level. Default level. ❑ High: The higher priority level. ❑ Crit: Critical, the highest priority level.

Table 23. SHOW POWER-INLINE Command (Continued)

Field	Description
Oper	The PoE operating status of the port. The possible status are listed here: ❐ Powered: The port is transmitting power to the PD. ❐ Denied: The port is not transmitting power to the PD because the switch has reached its maximum power capacity. ❐ Off: PoE is disabled on the port. ❐ Fault: The switch is exceeding the total available power. ❐ Test: The port is in a test mode.
Power	The port's current power consumption in milliwatts (mW).
Device	The port's PD description. This parameter is set with "POWER-INLINE DESCRIPTION" on page 267.
Class	The PD's class PD. See "PD Classes" on page 244 for details.
Max (mW)	The port's maximum power limit in milliwatts (mW) and how the limit was set. The methods are listed here: ❐ [U]: The power limit was set with "POWER-INLINE MAX" on page 269. ❐ [L]: The power limit was supplied by LLDP. ❐ [C]: The power limit was set according to the PD's class.

Example

This example displays PoE information about the switch and ports:

```
awplus# show power-inline
```

SHOW POWER-INLINE COUNTERS INTERFACE

Syntax

```
show power-inline counters interface port
```

Parameter

port
Specifies a port. You can specify and display more than one port at a time. Omit this parameter to display all of the ports.

Mode

Privileged Exec mode

Description

Use this command to display the PoE event counters for the ports. An example is shown in Figure 61.

```
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
```

Figure 61. SHOW POWER-INLINE COUNTERS INTERFACE Command

The fields are described in Table 24.

Table 24. SHOW POWER-INLINE COUNTERS INTERFACE Command

Field	Description
Interface	The port number.
Overload	The number of times the PD exceeded the power limit set with "POWER-INLINE MAX" on page 269.
Short	The number of short circuits the port has experienced.
Invalid	The number of times the port detected an invalid signature. An invalid signature indicates an open circuit, a short circuit, or a legacy PD.

Table 24. SHOW POWER-INLINE COUNTERS INTERFACE Command

Field	Description
Denied	The number of times the port had to deny power to the PD because the switch had reached its maximum power capacity.

Example

This command displays the PoE event counters for ports 4 to 6:

```
awplus# show power-inline counters interface port1.0.4-
port1.0.6
```

SHOW POWER-INLINE INTERFACE

Syntax

```
show power-inline interface port
```

Parameter

port
      Specifies a port. You can display more than one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display the PoE information on the ports. An example is shown in Figure 62.

```
Interface Admin     Pri   Oper      Power  Device  Class  Max(mW)
port1.0.1 Disabled Low   Disabled 0                0     15400 [C]
port1.0.2 Enabled  High  Powered  3840    Phone   1     5000 [U]
port1.0.3 Enabled  Crit  Powered  6720    AccessPt 2     7000 [C]
port1.0.4 Disabled Low   Disabled 0                0     15400 [C]
```

Figure 62. SHOW POWER-INLINE INTERFACE Command

This command displays a subset of the information the SHOW POWER-INLINE command displays. The fields are described in Table 23 on page 275.

Example

This example displays PoE information for ports 1 to 4:

```
awplus# show power-inline interface port1.0.1-port1.0.4
```

SHOW POWER-INLINE INTERFACE DETAIL

Syntax

```
show power-inline interface port detail
```

Parameter

port
> Specifies a port. You can display more than one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display additional information about the ports. An example is shown in Figure 63.

```
Interface port1.0.1
   Powered device type: Desk Phone #1
   PoE admin enabled
  Priority Low
   Detection status: Powered
   Current power consumption: 00 mW
   Powered device class: 1
   Power allocated: 5000 mW (from configuration)
   Detection of legacy devices is disabled
```
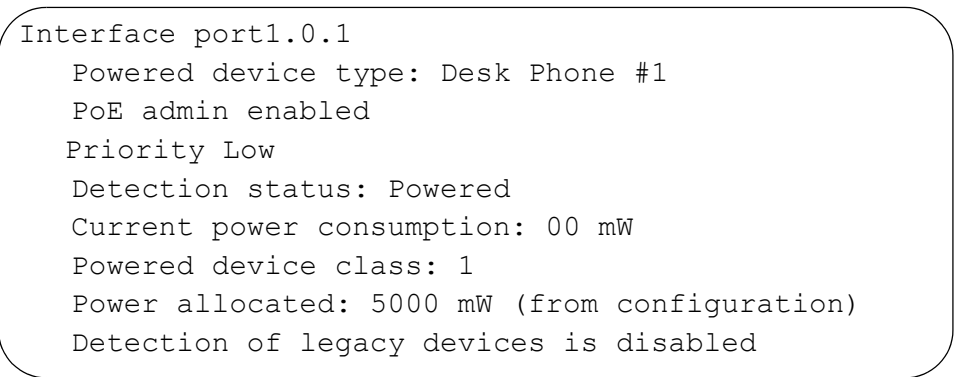
Figure 63. SHOW POWER-INLINE INTERFACE DETAIL Command

The fields are described in Table 25.

Table 25. SHOW POWER-INLINE INTERFACE DETAIL Command

Field	Description
Interface	The port number.
Powered device type	The PD description. The description is set with "POWER-INLINE DESCRIPTION" on page 267.

Table 25. SHOW POWER-INLINE INTERFACE DETAIL Command

Field	Description
PoE admin	The status of PoE on the port. The status can be one of the following: ❑ Enabled: PoE is enabled. The port can transmit power to a PD. PoE is enabled with "POWER-INLINE ENABLE" on page 268. ❑ Disabled: PoE is disabled. The port does not supply power to a PD, but it does forward network traffic. PoE is disabled with "NO POWER-INLINE ENABLE" on page 260.
Priority	The port's PoE priority level. The priority level is set with "POWER-INLINE PRIORITY" on page 270. The priorities are listed here: ❑ Low: the lowest priority level. This is default level. ❑ High: the higher priority level. ❑ Crit: the critical, or highest priority level.
Detection status	The PoE operating status of the port. The possible status are listed here: ❑ Powered: The port is transmitting power to the PD. ❑ Denied: The port is not transmitting power to the PD because the switch has reached its maximum power capacity. ❑ Off: PoE is disabled on the port. ❑ Fault: The switch is exceeding the total available power. ❑ Test: The port is in a test mode.
Current power consumption	The port's current power consumption in milliwatts (mW).
Powered device class	The PD's class. See "PD Classes" on page 244 for details.
Power allocated	The port's power limit in milliwatts (mW).

Table 25. SHOW POWER-INLINE INTERFACE DETAIL Command

Field	Description
Detection of legacy devices	The status of support for a legacy PD on the port: ❐ Enabled: The port supports legacy devices. ❐ Disabled: The port does not support legacy devices. Support for legacy devices is enabled with "POWER-INLINE ALLOW-LEGACY" on page 266 and disabled with "NO POWER-INLINE ALLOW-LEGACY" on page 258.
Powered pairs	The twisted pairs used to transfer power to the PD. This parameter is not adjustable. The value is one of the following: ❐ Data ❐ Spare

Examples

This example displays PoE information for port 1:

```
awplus# show power-inline interface port1.0.1 detail
```

This example displays PoE information for ports 7 to 10:

```
awplus# show power-inline interface port1.0.7-port1.0.10
detail
```

282

SNMP-SERVER ENABLE TRAP POWER-INLINE

Syntax

```
snmp-server enable trap power-inline
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the transmission of the SNMP power-inline trap. The trap is sent if the power requirements of the switch and PDs exceed the power limit threshold set with "POWER-INLINE USAGE-THRESHOLD" on page 272.

Confirmation Command

"SHOW RUNNING-CONFIG SNMP" on page 985

Example

This example enables the SNMP power-inline trap:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
```

Chapter 13

IPv4 and IPv6 Management Addresses

This chapter contains the following information:

Overview

This chapter explains how to assign the switch an IP address. The switch must have an IP address to perform the features in Table 26. It uses the address as its source address when it communicates with other network devices, such as TFTP servers, and Telnet management workstations.

You may assign the switch an IPv4 or IPv6 address, or both. The switch supports only one address of each version. The switch can support all of the features with an IPv4 address, but only a subset of the features with an IPv6 address. To use features that are not supported by an IPv6 address, you must assign the switch an IPv4 address instead of or along with an IPv6 address.

Table 26. Features Requiring an IP Management Address on the Switch

Feature	Description	Supported by IPv4 Address	Supported by IPv6 Address
802.1x port-based network access control	Used with a RADIUS server for port security.	yes	no
Enhanced stacking	Used to manage more than one switch from the same local or remote management session.	yes	no
Ping	Used to test for valid links between the switch and other network devices.	yes	yes
RADIUS client	Used for remote management authentication and for 802.1x port-based network access control.	yes	no
RMON	Used with the RMON portion of the MIB tree on an SNMP workstation to remotely monitor the switch.	yes	no
Secure Shell server	Used to remotely manage the switch with a Secure Shell client.	yes	yes
sFlow agent	Used to transmit packet statistics and port counters to an sFlow collector on your network.	yes	no

286

Table 26. Features Requiring an IP Management Address on the Switch (Continued)

Feature	Description	Supported by IPv4 Address	Supported by IPv6 Address
SNMPv1, v2c, and v3	Used to remotely manage the switch with SNMP.	yes	yes
SNTP client	Used to set the date and time on the switch from an NTP or SNTP server on your network or the Internet.	yes	no
Static ARP entries	Used to add static ARP entries to the switch.	yes	no
Syslog client	Used to send the event messages from the switch to syslog servers on your network for storage.	yes	no
TACACS+ client	Used for remote management authentication using a TACACS+ server on your network.	yes	no
Telnet client	Used to manage other network devices from the switch.	yes	yes
Telnet server	Used to remotely manage the switch with a Telnet client.	yes	yes
TFTP client	Used to download files to or upload files from the switch using a TFTP server.	yes	yes
Non-secure HTTP web browser server	Used to remotely manage the switch with a web browser.	yes	yes
Secure HTTPS web browser server	Used to remotely manage the switch with a web browser, with encryption.	yes	yes

Here are the guidelines to assigning the switch management IPv4 and IPv6 addresses:

❒ The switch supports one IPv4 address and one IPv6 address.

❒ A management address can be assigned to a VLAN on the switch. It can be assigned to any VLAN, including the Default_VLAN. For background information on VLANs, refer to Chapter 47, "Port-based and Tagged VLANs" on page 717.

❐ If you assign both IPv4 and IPv6 addresses to the switch, they must be assigned to the same VLAN.

❐ An IPv4 management address can be assigned manually or from a DHCP server on your network. (To learn the switch's MAC address to add to a DHCP server, refer to "SHOW SWITCH" on page 159.)

❐ An IPv6 address must be assigned manually. The switch does not support the assignment of an IPv6 management address from a DHCP server or by IPv6 auto assignment.

❐ You must also assign the switch a default gateway if the management devices (syslog servers, Telnet workstations, etc,) are not members of the same subnet as the management address. This IP address designates an interface on a router or other Layer 3 device that represents the first hop to the remote subnets or networks where the network devices are located.

❐ The default gateway address, if needed, must be a member of the same subnet as the management address.

288

Assigning an IPv4 Management Address and Default Gateway

This section covers the following topics:

❐ "Adding an IPv4 Management Address" next

❐ "Adding an IPv4 Default Gateway Address" on page 291

❐ "Deleting an IPv4 Management Address and Default Gateway" on page 292

❐ "Displaying an IPv4 Management Address and Default Gateway" on page 293

Adding an IPv4 Management Address

The command to assign the switch an IPv4 management address is the IP ADDRESS command. It has to be performed from the VLAN Configuration mode of the VLAN to which the address is to be assigned. If the VLAN does not already exist, you have to create it before you can assign the address. For instructions, refer to Chapter 47, "Port-based and Tagged VLANs" on page 717.

Here is the format of the command:

```
ip address ipaddress/mask|dhcp
```

The IPADDRESS parameter is the IPv4 management address to be assigned the switch. The address is specified in this format:

nnn.nnn.nnn.nnn

Each NNN is a decimal number from 0 to 255. The numbers must be separated by periods.

The MASK parameter is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. Here are a couple of basic examples:

❐ The decimal mask 16 is equivalent to the mask 255.255.0.0.

❐ The decimal mask 24 is equivalent to the mask 255.255.255.0.

Note
If a management IPv4 address is already assigned to the switch, you must delete it before entering a new address. For instructions, refer to "Deleting an IPv4 Management Address and Default Gateway" on page 292.

Here are several examples of the command. The first example assigns the switch the management IPv4 address 149.121.43.56/24 to the Default_VLAN, which has the VID number 1.

> **Note**
> By default, the switch is configured with the Default_VLAN which has a VID number of 1 and includes all ports on the switch. The Default_VLAN only has default values and cannot be created, modified or deleted.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 149.121.43.56/24
awplus(config-if)# exit
```

This example assigns the IPv4 management address 143.24.55.67 and subnet mask 255.255.255.0 to a new VLAN titled Tech_support. The VLAN is assigned the VID 17 and consists of untagged ports 5 and 6. The first series of commands create the new VLAN.

`awplus> enable`	Enter the Privileged Executive mode from the User Exec mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# vlan database`	Use the VLAN DATABASE command to enter the VLAN Configuration mode.
`awplus(config-vlan)# vlan 17 name Tech_support`	Use the VLAN command to assign the VID 17 and the name Tech_support to the new VLAN.
`awplus(config-vlan)# exit`	Return to the Global Configuration mode.
`awplus(config)# interface port1.0.5,port1.0.6`	Enter the Port Interface mode for ports 5 and 6.
`awplus(config-if)# switchport access vlan 17`	Use the SWITCHPORT ACCESS VLAN command to add the ports to the new VLAN.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan`	Use the SHOW VLAN command to confirm the configuration of the new VLAN.

The next series of commands assigns the management address 143.24.55.67 and subnet mask 255.255.255.0 to the new VLAN.

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface vlan17`	Use the INTERFACE VLAN command to move to the VLAN Interface.
`awplus(config-if)# ip address 143.24.55.67/24`	Use the IP ADDRESS command to assign the management address 143.24.55.67 and subnet mask 255.255.255.0 to the VLAN.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show ip interface`	Use the SHOW IP INTERFACE command to display the new management IPv4 address.

This example activates the DHCP client so that the management IPv4 address is assigned to the Default_VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address dhcp
```

Adding an IPv4 Default Gateway Address

The switch must be assigned a default gateway if the management devices (for example, syslog servers, TFTP servers, and Telnet clients) are not members of the same subnet as the management IPv4 address. A default gateway is an IP address of an interface on a router or other Layer 3 device. It represents the first hop to the networks in which the management devices reside. The switch can have only one IPv4 default gateway and the address must be a member of the same subnet as the management IPv4 address.

The command for assigning the default gateway is the IP ROUTE command in the Global Configuration mode. Here is the format:

`ip route 0.0.0.0/0` *ipaddress*

The IPADDDRESS parameter is the default gateway to be assigned the switch.

Note
If an IPv4 default gateway is already assigned to the switch, you must delete it prior to entering the new address. For instructions, refer to "Deleting an IPv4 Management Address and Default Gateway" on page 292.

This example assigns the switch the default gateway address 149.121.43.23:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip route 0.0.0.0/0 149.121.43.23
```

To verify the default route, issue these commands:

```
awplus(config)# exit
awplus# show ip route
```

For information about how to add static IPv4 routes, see "Adding Static and Default Routes" on page 1806.

Deleting an IPv4 Management Address and Default Gateway

The switch does not allow you to make any changes to the current management address on the switch. If you want to change the address or assign it to a different VLAN, you have to delete it and recreate it, with the necessary changes.

To delete a static IPv4 management address from the switch, enter the NO IP ADDRESS command in the VLAN Interface mode in which the current address is assigned. This example of the command deletes the address from a VLAN with the VID of 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan17
awplus(config-if)# no ip address
```

To delete an IPv4 management address assigned by a DHCP server, use the NO IP ADDRESS DHCP command. This example of the command deletes the management address assigned by a DHCP server, from a VLAN on the switch with the VID of 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan23
awplus(config-if)# no ip address dhcp
```

To remove the current default gateway, use the NO form of the IP ROUTE command. The command must include the current default gateway. This example removes the default route 149.121.43.23:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip route 0.0.0.0/0 149.121.43.23
```

Displaying an IPv4 Management Address and Default Gateway

The easiest way to view the IPv4 management address and default gateway address of the switch is with the SHOW IP ROUTE command. It displays both addresses at the same time. The command is found in the Privileged Exec mode, as shown here:

```
awplus# show ip route
```

See Figure 64 for an example of the information. The management IPv4 address of the switch is displayed in the first entry in the table and the default gateway address, if assigned to the switch, in the second entry. Figure 64 displays an example of the information.

```
-------------------------------------------------------------------
Destination     Mask           NextHop         Interface   Protocol
-------------------------------------------------------------------
192.168.1.0     255.255.255.0  192.168.1.1     vlan1-0     INTERFACE
-------------------------------------------------------------------
```

Figure 64. SHOW IP ROUTE Command

The columns in the display are defined in Table 28 on page 318.

To view only the management IP address, use the SHOW IP INTERFACE command, also in the Privileged Exec mode:

```
awplus# show ip interface
```

Here is an example of the information from the command.

```
Interface       IP Address       Status        Protocol
VLAN14-0        123.94.146.72    admin up      down
```

Figure 65. SHOW IP INTERFACE Command

For definitions of the columns: See "SHOW IP INTERFACE" on page 317.

Assigning an IPv6 Management Address and Default Gateway

This section covers the following topics:

❒ "Adding an IPv6 Management Address" next

❒ "Adding an IPv6 Default Gateway Address" on page 295

❒ "Deleting an IPv6 Management Address and Default Gateway" on page 296

❒ "Displaying an IPv6 Management Address and Default Gateway" on page 297

Adding an IPv6 Management Address

The command to assign the switch an IPv6 management address is the IPv6 ADDRESS command. As with the IPv4 address command, this command has to be performed in the VLAN Configuration mode of the VLAN to which the address is to be assigned. If the VLAN does not already exist, you have to create it first. For instructions, refer to Chapter 47, "Port-based and Tagged VLANs" on page 717. If the switch already has an IPv4 address, the IPv6 address must be assigned to the same VLAN as that address.

Here is the format of the command:

```
ipv6 address ipaddress/mask
```

The IPADDRESS parameter is the management IPv6 address for the switch, entered in this format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where N is a hexadecimal digit from 0 to F. The eight groups of digits are separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

12c4:421e:09a8:0000:0000:0000:00a4:1c50

12c4:421e:9a8::a4:1c50

The MASK parameter is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. For example, an address whose network designator consists of the first eight bytes would need a mask of 64 bits.

> **Note**
> If there is a management IPv6 address already assigned to the switch, you must delete it prior to entering the new address. For instructions, refer to "Deleting an IPv6 Management Address and Default Gateway" on page 296.

Here are several examples of the command. The first example assigns the switch this static management IPv6 address to the Default_VLAN with VID number 1.

90:0a21:091b:0000:0000:0000:09bd:c458

Here are the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 address 90:a21:91b::9bd:c458/64
awplus(config-if)# exit
```

This example assigns a management IPv6 address to a VLAN with the VID 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan8
awplus(config-if)# ipv6 address 1857:80cf:d54::1a:8f57/64
awplus(config-if)# exit
```

> **Note**
> You cannot use a DHCP server or SLAAC (State Address Autoconfiguration) to assign the switch a dynamic IPv6 address. The switch supports only a single static IPv6 address.

Adding an IPv6 Default Gateway Address

The switch must be assigned a default gateway if the management devices (for example, TFTP servers, Telnet clients and SSH clients) are not members of the same subnet as its management IPv6 address. A default gateway is an IP address of an interface on a router or other Layer 3 device that is the first hop to the networks in which the management devices are located. The switch can have only one IPv6 default gateway and the address must be a member of the same subnet as the management IPv6 address.

The command for assigning the default gateway is the IPV6 ROUTE command in the Global Configuration mode. Here is the format of the command:

```
ipv6 route ::/0 ipaddress
```

The IPADDDRESS parameter is the default gateway to be assigned the switch. The address must be an IPv6 address and it must be a member of the same subnet as the management IPv6 address.

> **Note**
> This configuration is different in the AT-8000GS switch where the gateway is specified as the Link Local address.

> **Note**
> If there is an IPv6 default gateway already assigned to the switch, you must delete it prior to entering the new default gateway. For instructions, refer to "Deleting an IPv6 Management Address and Default Gateway" on page 296.

This example assigns the switch the default gateway address 389c:be45:78::c45:8156:

```
awplus> enable
awplus# configure terminal
awplus(config)# ipv6 route ::/0 389c:be45:78::c45:8156
```

To verify the default route, issue these commands:

```
awplus(config-if)# end
awplus# show ipv6 route
```

Deleting an IPv6 Management Address and Default Gateway

To delete a static IPv6 management address, enter the NO IPV6 ADDRESS command in the VLAN Interface mode in which the current address is assigned. This example of the command deletes the address from a VLAN with the VID 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan21
awplus(config-if)# no ipv6 address
```

To remove the default gateway, use the NO form of the IPV6 ROUTE command. The command must include the current default gateway. Here is the format of the command:

```
no ipv6 route ::/0 ipaddress
```

The IPADDRESS parameter specifies the default route to be deleted. This example deletes the default route 389c:be45:78::c45:8156:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ipv6 route ::/0 389c:be45:78::c45:8156
```

Displaying an IPv6 Management Address and Default Gateway

There are two commands for displaying a management IPv6 address and default gateway. If the switch has both an IPv6 address and default gateway, you can display both of them with the SHOW IPV6 ROUTE command, in the Privileged Exec mode, as shown here:

```
awplus# show ipv6 route
```

Here is an example of the information. The default route is displayed first, followed by the management address.

```
IPv6 Routing Table
Codes: C - connected, S - static

S    0:0:0:0:0:0:0:0/0 via 832a:5821:b34a:0:0:0:187:14, vlan4-0

C    832a:5821:b34a:0:0:0:187:95a/64 via ::, vlan4-0
```

Figure 66. SHOW IPV6 ROUTE Command

Another way to display just the management address is with the SHOW IPV6 INTERFACE command, shown here:

```
awplus# show ipv6 interface
```

Here is an example of the information from the command.

```
Interface       IPv6-Address                          Status      Protocol
VLAN3-0         832a:5821:b34a:0:0:0:187:95a/64       admin up    down
```

Figure 67. SHOW IPV6 INTERFACE Command

The columns are defined in Table 29 on page 320.

298

Chapter 14

IPv4 and IPv6 Management Address Commands

The IPv4 and IPv6 management address commands are summarized in Table 27.

Table 27. Management IP Address Commands

Command	Mode	Description
"CLEAR IPV6 NEIGHBORS" on page 301	Privileged Exec	Clears all dynamic IPv6 neighbor entries.
"IP ADDRESS" on page 302	VLAN Interface	Assigns the switch a static IPv4 management address.
"IP ADDRESS DHCP" on page 304	VLAN Interface	Assigns the switch an IPv4 management address from a DHCP server on your network.
"IP ROUTE" on page 306	Global Configuration	Assigns the switch an IPv4 default gateway address.
"IPV6 ADDRESS" on page 308	VLAN Interface	Assigns the switch a static IPv6 management address.
"IPV6 ROUTE" on page 310	Global Configuration	Assigns the switch an IPv6 default gateway address.
"NO IP ADDRESS" on page 312	VLAN Interface	Deletes the IPv4 management address.
"NO IP ADDRESS DHCP" on page 313	VLAN Interface	Deactivates the IPv4 DHCP client on the switch.
"NO IP ROUTE" on page 314	Global Configuration	Deletes the IPv4 default gateway.
"NO IPV6 ADDRESS" on page 315	VLAN Interface	Deletes the IPv6 management address.
"NO IPV6 ROUTE" on page 316	Global Configuration	Deletes the IPv6 default gateway.
"SHOW IP INTERFACE" on page 317	Privileged Exec	Displays the IPv4 management address.
"SHOW IP ROUTE" on page 318	Privileged Exec	Displays the IPv4 management address and default gateway.

Table 27. Management IP Address Commands (Continued)

Command	Mode	Description
"SHOW IPV6 INTERFACE" on page 320	Privileged Exec	Displays the IPv4 management address.
"SHOW IPV6 ROUTE" on page 321	Privileged Exec	Displays the IPv6 management address and default gateway.

CLEAR IPV6 NEIGHBORS

Syntax

```
clear ipv6 neighbors
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to clear all of the dynamic IPv6 neighbor entries.

Example

This example clears all of the dynamic IPv6 neighbor entries:

```
awplus> enable
awplus# clear ipv6 neighbors
```

IP ADDRESS

Syntax

```
ip address ipaddress/mask
```

Parameters

ipaddress
> Specifies a management IPv4 address for the switch. The address is specified in the following format:
>
> nnn.nnn.nnn.nnn
>
> Where each NNN is a decimal number from 0 to 255. The numbers must be separated by periods.

mask
> Specifies the subnet mask for the address. The mask is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. For example, the IPv4 decimal masks 16 and 24 are equivalent to masks 255.255.0.0 and 255.255.255.0, respectively.

Mode

VLAN Interface mode

Description

Use this command to manually assign the switch an IPv4 management address. You must perform this command from the VLAN Interface mode of the VLAN to which to the address is to be assigned.

To assign the switch an IPv4 address from a DHCP server, refer to "IP ADDRESS DHCP" on page 304.

An IPv4 management address is required to support the features listed in Table 26 on page 286. The switch can have only one IPv4 address, and it must be assigned to the VLAN from which the switch is to communicate with the management devices (such as Telnet workstations and syslog servers). The VLAN must already exist on the switch before you use this command.

Confirmation Command

"SHOW IP INTERFACE" on page 317

Examples

This example assigns the switch the IPv4 management address 142.35.78.21 and subnet mask 255.255.255.0. The address is assigned to the Default_VLAN, which has the VID 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 142.35.78.21/24
```

This example assigns the switch the IPv4 management address 116.152.173.45 and subnet mask 255.255.255.0. The VLAN assigned the address has the VID 14:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan14
awplus(config-if)# ip address 116.152.173.45/24
```

IP ADDRESS DHCP

Syntax

```
ip address dhcp
```

Parameters

None

Mode

VLAN Interface mode

Description

Use this command to assign the switch an IPv4 management address from a DHCP server. This command activates the DHCP client, which automatically queries the network for a DHCP server. The client also queries for a DHCP server whenever you reset or power cycle the switch.

You must perform this command from the VLAN Interface mode of the VLAN to which you want to assign the address.

The switch must have a management IPv4 address to support the features listed in Table 26 on page 286. The switch can have only one IPv4 address, and it must be assigned to the VLAN from which the switch is to communicate with the management devices (such as Telnet workstations and syslog servers). The VLAN must already exist on the switch.

To manually assign the switch an IPv4 address, refer to "IP ADDRESS" on page 302.

Note
You cannot assign the switch a dynamic IPv6 address from a DHCP server. An IPv6 management address must be assigned manually with "IPV6 ADDRESS" on page 308.

Confirmation Commands

"SHOW IP INTERFACE" on page 317 and "SHOW IP ROUTE" on page 318

304

Example

This example activates the DHCP client so that the switch obtains its IPv4 management address from a DHCP server on your network. The address is applied to a VLAN with the VID 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip address dhcp
```

IP ROUTE

Syntax

```
ip route 0.0.0.0/0 ipaddress
```

Parameters

ipaddress
>Specifies an IPv4 default gateway address.

Mode

Global Configuration mode

Description

Use this command to assign the switch an IPv4 default gateway address. A default gateway is an address of an interface on a router or other Layer 3 device. The switch uses the address as the first hop to reaching remote subnets or networks when communicating with management network devices, such as Telnet clients and syslog servers, that are not members of the same subnet as its IPv4 address.

You must assign the switch a default gateway address if both of the following are true:

❏ You assigned the switch an IPv4 management address.

❏ The management network devices are not members of the same subnet as the management IP address.

Review the following guidelines before assigning a default gateway address to the switch:

❏ The switch can have just one IPv4 default gateway address.

❏ The switch must already have an IPv4 management address.

❏ The management address and the default gateway address must be members of the same subnet.

Confirmation Command

"SHOW IP ROUTE" on page 318

Example

This example assigns the switch the IPv4 default gateway address 143.87.132.45:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip route 0.0.0.0/0 143.87.132.45
```

IPV6 ADDRESS

Syntax

```
ipv6 address ipaddress/mask
```

Parameters

ipaddress

Specifies an IPv6 management address for the switch. The address is entered in this format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where N is a hexadecimal digit from 0 to F. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

12c4:421e:09a8:0000:0000:0000:00a4:1c50

12c4:421e:9a8::a4:1c50

mask

Specifies the subnet mask of the address. The mask is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. For example, an address whose network designator consists of the first eight bytes would need a mask of 64 bits.

Mode

VLAN Interface mode

Description

Use this command to manually assign the switch an IPv6 management address. You must perform this command from the VLAN Interface mode of the VLAN to which to the address is to be assigned.

> **Note**
> An IPv6 management address must be assigned manually. The switch cannot obtain an IPv6 address from a DHCP server.

The switch must have a management address to support the features listed in Table 26 on page 286. The switch can have only one IPv6 address, and it must be assigned to the VLAN from which the switch is to communicate with the management devices (such as Telnet workstations

308

and syslog servers). The VLAN must already exist on the switch before you use this command.

Confirmation Commands

"SHOW IPV6 INTERFACE" on page 320 and "SHOW IPV6 ROUTE" on page 321

Examples

This example assigns the IPv6 management address 4c57:17a9:11::190:a1d4/64 to the Default_VLAN, which has the VID 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 address 4c57:17a9:11::190:a1d4/64
```

This example assigns the switch the IPv6 management IPv4 address 7891:c45b:78::96:24/64 to a VLAN with the VID 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 address 7891:c45b:78::96:24/64
```

IPV6 ROUTE

Syntax

```
ipv6 route ::/0 ipaddress
```

Parameters

ipaddress

Specifies an IPv6 address of a default gateway. The address is entered in this format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where N is a hexadecimal digit from 0 to F. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted.

Mode

Global Configuration mode

Description

Use this command to assign the switch an IPv6 default gateway address. A default gateway is an address of an interface on a router or other Layer 3 device. It defines the first hop to reaching the remote subnets or networks where the network devices are located. You must assign the switch a default gateway address if both of the following are true:

❐ You assigned the switch an IPv6 management address.

❐ The remote management devices (such as Telnet workstations and TFTP servers) are not members of the same subnet as the IPv6 management address.

Review the following guidelines before assigning a default gateway address:

❐ The switch can have just one IPv6 default gateway.

❐ The switch must already have an IPv6 management address.

❐ The IPv6 management address and the default gateway address must be members of the same subnet.

Confirmation Command

"SHOW IPV6 ROUTE" on page 321

310

Example

This example assigns the switch the IPv6 default gateway address 45ab:672:934c::78:17cb:

```
awplus> enable
awplus# configure terminal
awplus(config)# ipv6 route ::/0 45ab:672:934c::78:17cb
```

NO IP ADDRESS

Syntax

```
no ip address
```

Parameters

None

Mode

VLAN Interface mode

Description

Use this command to delete the current IPv4 management address from the switch if the address was assigned manually. If a DHCP server supplied the address, refer to "NO IP ADDRESS DHCP" on page 313. You must perform this command from the VLAN Interface mode of the VLAN to which the address is attached.

Note
The switch uses the IPv4 management address to perform the features listed Table 26 on page 286. If you delete it, the switch will not support the features unless it also has an IPv6 management address.

Confirmation Commands

"SHOW IP INTERFACE" on page 317 and "SHOW IP ROUTE" on page 318

Example

This example removes the static IPv4 management address from the VLAN with the VID 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# no ip address
```

312

NO IP ADDRESS DHCP

Syntax

```
no ip address dhcp
```

Parameters

None

Mode

VLAN Interface mode

Description

Use this command to delete the current IPv4 management address from the switch if the address was assigned by a DHCP server. You must perform this command from the VLAN Interface mode of the VLAN to which the address is attached. This command also disables the DHCP client.

Note
The switch uses the IPv4 management address to perform the features listed Table 26 on page 286. If you delete it, the switch will not support the features unless it also has an IPv6 management address.

Confirmation Command

"SHOW IP INTERFACE" on page 317 and "SHOW IP ROUTE" on page 318

Example

This example removes the IPv4 management address from a VLAN with the VID 3 and disables the DHCP client:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip address dhcp
```

313

NO IP ROUTE

Syntax

```
no ip route 0.0.0.0/0 ipaddress
```

Parameters

ipaddress
    Specifies the current default gateway.

Mode

Global Configuration mode

Description

Use this command to delete the current IPv4 default gateway. The command must include the current default gateway.

Confirmation Command

"SHOW IP ROUTE" on page 318

Example

This example deletes the default route 121.114.17.28 from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip route 0.0.0.0/0 121.114.17.28
```

NO IPV6 ADDRESS

Syntax

```
no ipv6 address
```

Parameters

None

Mode

VLAN Interface mode

Description

Use this command to delete the current IPv6 management address from the switch. You must perform this command from the VLAN Interface mode of the VLAN to which the address is attached.

> **Note**
> The switch uses the IPv6 management address to perform the features listed Table 26 on page 286. If you delete it, the switch will not support the features unless it also has an IPv4 management address.

Confirmation Command

"SHOW IPV6 INTERFACE" on page 320 and "SHOW IPV6 ROUTE" on page 321

Example

This example removes the static IPv6 management address from the VLAN with the VID 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ipv6 address
```

NO IPV6 ROUTE

Syntax

```
no ipv6 route ::/0 ipaddress
```

Parameters

ipaddress
> Specifies the current IPv6 default gateway.

Mode

Global Configuration mode

Description

Use this command to delete the current IPv6 default gateway from the switch. The command must include the current default gateway.

Confirmation Command

"SHOW IPV6 ROUTE" on page 321

Example

This example deletes the IPv6 default route 2b45:12:9ac4::5bc7:89 from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ipv6 route ::/0 2b45:12:9ac4::5bc7:89
```

SHOW IP INTERFACE

Syntax

```
show ip interface
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the management IP address on the switch. Figure 68 is an example of the information.

```
Interface      IP Address
VLAN14-0       123.94.146.72
```

Figure 68. SHOW IP INTERFACE Command

The Interface field is the VID of the VLAN to which the management IP address is assigned. The IP Address field is the management IP address of the switch.

Example

The following example displays the management IP address assigned to a switch:

```
awplus# show ip interface
```

SHOW IP ROUTE

Syntax

```
show ip route
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the routes on the switch. Figure 69 displays an example of the information.

```
----------------------------------------
 Mask             NextHop        Interface
----------------------------------------
 255.255.255.0   192.168.1.1     vlan1-0
----------------------------------------
```

Figure 69. SHOW IP ROUTE Command

The fields are described in Table 28.

Table 28. SHOW IP ROUTE Command

Parameter	Description
Mask	The masks of the management IP address and the default gateway address. The mask of the default gateway is always 0.0.0.0.
NextHop	The management IP address and the default gateway address. The management IP address is the first entry in the table, and the default gateway address is the second entry.
Interface	The VID of the VLAN to which the management IP address is assigned.

Example

The following example displays the routes on the switch:

```
awplus# show ip route
```

SHOW IPV6 INTERFACE

Syntax

```
show ipv6 interface
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the IPv6 management address on the switch. Figure 70 is an example of the information.

```
Interface      IPv6-Address
VLAN3-0        832a:5821:b34a:0:0:0:187:95a/64
```

Figure 70. SHOW IPV6 INTERFACE Command

The fields are described in Table 29.

Table 29. SHOW IPV6 INTERFACE Command

Parameter	Description
Interface	The VID of the VLAN to which the management address is assigned.
IPv6 Address	The IPv6 management address of the switch.

Example

The following example displays the IPv6 management address:

```
awplus# show ipv6 interface
```

SHOW IPV6 ROUTE

Syntax

```
show ipv6 route
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the IPv6 management address and default gateway on the switch. Figure 71 is an example of the information. The default route is display first, followed by the management address.

```
IPv6 Routing Table
Codes: C - connected, S - static

S    0:0:0:0:0:0:0:0/0 via 832a:5821:b34a:0:0:0:187:14, vlan4-0

C    832a:5821:b34a:0:0:0:187:95a/64 via ::, vlan4-0
```

Figure 71. SHOW IPV6 ROUTE Command

Example

The following example displays the IPv6 management address and default gateway:

```
awplus# show ipv6 route
```

321

Chapter 15

Simple Network Time Protocol (SNTP) Client

This chapter contains the following information:

Overview

The switch has a Simple Network Time Protocol (SNTP) client for setting its date and time from an SNTP or NTP server on your network or the Internet. The date and time are added to the event messages that are stored in the event log and sent to syslog servers.

The switch polls the SNTP or NTP server for the date and time when you configure the client and when the unit is powered on or reset.

Here are the guidelines to using the SNTP client:

❑ You must specify the IP address of the SNTP or NTP server from which the switch is to obtain the date and time. You can specify only one IP address. For instructions, refer to "Activating the SNTP Client and Specifying the IP Address of an NTP or SNTP Server" on page 325.

❑ You must configure the client by specifying whether the locale of the switch is in Standard Time or Daylight Savings Time. For instructions, refer to "Configuring Daylight Savings Time and UTC Offset" on page 326.

❑ You must specify the offset of the switch from Coordinated Universal Time (UTC). For instructions, refer to "Configuring Daylight Savings Time and UTC Offset" on page 326.

❑ The switch must have a management IP address to communicate with an SNTP or NTP server. For instructions, refer to "Adding a Management IP Address" on page 72 or Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❑ The SNTP or NTP server must be a member of the same subnet as the management IP address of the switch or be able to access it through routers or other Layer 3 devices.

❑ If the management IP address of the switch and the IP address of the SNTP or NTP server are members of different subnets or networks, you must also assign the switch a default gateway. This is the IP address of a routing interface that represents the first hop to reaching the remote network of the SNTP or NTP server. For instructions, refer to "Adding a Management IP Address" on page 72 or Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

Activating the SNTP Client and Specifying the IP Address of an NTP or SNTP Server

To activate the SNTP client on the switch and to specify the IP address of an NTP or SNTP server, use the NTP PEER command in the Global Configuration mode. You can specify the IP address of only one server.

This example of the command specifies 1.77.122.54 as the IP address of the server:

```
awplus> enable
awplus# configure terminal
awplus(config)# ntp peer 1.77.122.54
```

To display the date and time, use the SHOW CLOCK command in the User Exec and Privileged Exec modes.

```
awplus# show clock
```

Configuring Daylight Savings Time and UTC Offset

If the time that the NTP or SNTP server provides to the switch is in Coordinated Universal Time (UTC), it has to be converted into local time. To do that, the switch needs to know whether to use Standard Time (ST) or Daylight Savings Time (DST), and the number of hours and minutes it is ahead of or behind UTC, referred to as the UTC offset.

> **Note**
> To set the daylight savings time and UTC offset, you must first specify the IP address of an NTP server with the NTP PEER command. For instructions, refer to "Activating the SNTP Client and Specifying the IP Address of an NTP or SNTP Server" on page 325.

This table lists the commands you use to configure the daylight savings time and UTC offset.

Table 30. SNTP Daylight Savings Time and UTC Offset Commands

To	Use This Command	Range
Configure the client for Daylight Savings Time	CLOCK SUMMER-TIME	-
Configure the client for Standard Time.	NO CLOCK SUMMER-TIME	-
Configure the UTC offset.	CLOCK TIMEZONE +*hh:mm*|-*hh:mm*	+12 to -12 hours in increments of 15. (The hours and minutes must each have two digits.)

The commands are located in the Global Configuration mode. This example configures the client for DST and a UTC offset of -8 hours:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock summer-time
awplus(config)# clock timezone -08:00
```

In this example, the client is configured for ST and a UTC offset of +2 hours and 45 minutes:

```
awplus> enable
awplus# configure terminal
awplus(config)# no clock summer-time
awplus(config)# clock timezone +02:45
```

327

Disabling the SNTP Client

To disable the SNTP client so that the switch does not obtain its date and time from an NTP or SNTP server, use the NO PEER command in the Global Configuration mode:
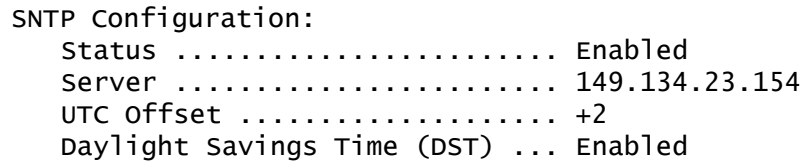
```
awplus> enable
awplus# configure terminal
awplus(config)# no ntp peer
```

Displaying the SNTP Client

To display the settings of the SNTP client on the switch, use the SHOW NTP ASSOCIATIONS command in the Privileged Exec mode.

awplus# show ntp associations

The following is displayed:
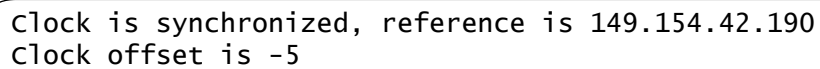
```
SNTP Configuration:
    Status ........................ Enabled
    Server ........................ 149.134.23.154
    UTC Offset .................... +2
    Daylight Savings Time (DST) ... Enabled
```

Figure 72. SHOW NTP ASSOCIATIONS Command

The fields are described in Table 32 on page 339.

To learn whether the switch has synchronized its time with the designated NTP or SNTP server, use the SHOW NTP STATUS command. An example of the information is shown in Figure 73.

```
Clock is synchronized, reference is 149.154.42.190
Clock offset is -5
```

Figure 73. SHOW NTP STATUS Command

329

Displaying the Date and Time

To display the date and time, use the SHOW CLOCK command in the User Exec mode or Privileged Exec mode:

```
awplus# show clock
```

Chapter 16
SNTP Client Commands

The SNTP commands are summarized in Table 31.

Table 31. Simple Network Time Protocol Commands

Command	Mode	Description
"CLOCK SUMMER-TIME" on page 332	Global Configuration	Activates Daylight Savings Time on the SNTP client.
"CLOCK TIMEZONE" on page 333	Global Configuration	Sets the UTC offset value, the time difference in hours and minutes between local time and Coordinated Universal Time (UTC).
"NO CLOCK SUMMER-TIME" on page 334	Global Configuration	Deactivates Daylight Savings Time and enables Standard Time.
"NO NTP PEER" on page 335	Global Configuration	Disables the NTP client.
"NTP PEER" on page 336	Global Configuration	Specifies the IP address of the NTP or SNTP server from which the switch is to obtain the date and time.
"PURGE NTP" on page 337	Global Configuration	Restores the default settings to the SNTP client.
"SHOW CLOCK" on page 338	User Exec and Privilege Exec	Displays the date and time.
"SHOW NTP ASSOCIATIONS" on page 339	Privilege Exec	Displays the settings of the NTP client on the switch.
"SHOW NTP STATUS" on page 341	Privilege Exec	Displays whether the switch has synchronized its time with the specified NTP or SNTP server.

CLOCK SUMMER-TIME

Syntax

```
clock summer-time
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable Daylight Savings Time (DST) on the SNTP client.

Note
The switch does not set the DST automatically. If the switch is in a locale that uses DST, you must remember to enable this when DST begins and disable when DST ends. If the switch is in a locale that does not use DST, set this option to disabled all the time. To disable DST on the client, refer to "NO CLOCK SUMMER-TIME" on page 334.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 339

Example

The following example enables DST on the SNTP client:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock summer-time
```

CLOCK TIMEZONE

Syntax

```
clock timezone +hh:mm|-hh:mm
```

Parameters

hh:mm

> Specifies the number of hours and minutes difference between Coordinated Universal Time (UTC) and local time. HH are hours in the range of -12 to +12, and MM are minutes in the range of increments of 15. The value is specified as ahead of (positive) or behind (negative) UTC. You must include both the hours and minutes, and both must have two digits. The default is 00:00.

Mode

Global Configuration mode

Description

Use this command to set the UTC offset, which is used by the switch to convert the time from an SNTP or NTP server into local time. You must configure the NTP client with "NTP PEER" on page 336 before setting the UTC offset.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 339

Examples

This example specifies a time difference of -2 hours between UTC and local time:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock timezone -02:00
```

This example specifies a time difference of +4 hours and 15 minutes between UTC and local time:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock timezone +04:15
```

NO CLOCK SUMMER-TIME

Syntax

```
no clock summer-time
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable Daylight Savings Time (DST) and activate Standard Time (ST) on the SNTP client.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 339

Examples

The following example disables Daylight Savings Time (DST) and activates Standard Time (ST) on the SNTP client:

```
awplus> enable
awplus# configure terminal
awplus(config)# no clock summer-time
```

NO NTP PEER

Syntax

```
no ntp server
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to deactivate the SNTP client on the switch. When the client is disabled, the switch does not obtain its date and time from an SNTP or NTP server the next time it is reset or power cycled.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 339

Example

The following example deactivates the SNTP client on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ntp peer
```

NTP PEER

Syntax

```
ntp peer ipaddress
```

Parameter

ipaddress
> Specifies an IP address of an SNTP or NTP server.

Mode

Global Configuration mode

Description

Use this command to activate the NTP client on the switch and to specify the IP address of the SNTP or NTP server from which it is to obtain its date and time. You can specify only one SNTP or NTP server. After you enter this command, the switch automatically begins to query the network for the defined server.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 339

Example

This example defines the IP address of the SNTP server as 1.77.122.54:

```
awplus> enable
awplus# configure terminal
awplus(config)# ntp peer 1.77.122.54
```

PURGE NTP

Syntax

```
purge ntp
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to disable the SNTP client, delete the IP address of the SNTP or NTP server, and restore the client settings to the default values.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 339

Example

The following example disables the SNTP client, deletes the IP address of the SNTP or NTP server, and restores the client settings to the default values:

```
awplus> enable
awplus# configure terminal
awplus(config)# purge ntp
```

SHOW CLOCK

Syntax

```
show clock
```

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display the switch's date and time.

Example

The following example displays the switch's date and time.

```
awplus# show clock
```

338

SHOW NTP ASSOCIATIONS

Syntax

```
show ntp associations
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the settings of the SNTP client. The information the command displays is shown in Figure 74.

```
NTP Configuration:
    Status ....................... Enabled
    Server ....................... 192.168.20.27
    UTC Offset ................... +02:00
    Daylight Savings Time (DST) ... Enabled
```

Figure 74. SHOW NTP ASSOCIATIONS Command

The information is described here:

Table 32. SHOW NTP ASSOCIATIONS Command

Parameter	Description
Status	The status of the SNTP client software on the switch. The status can be either enabled or disabled. If enabled, the switch seeks its date and time from an NTP or SNTP server. The default is disabled. To enable the client, use "NTP PEER" on page 336. To disable the client, refer to "NO NTP PEER" on page 335.
Server	The IP address of an NTP or SNTP server. This value is set with "NTP PEER" on page 336.

Table 32. SHOW NTP ASSOCIATIONS Command (Continued)

Parameter	Description
UTC Offset	The time difference in hours between UTC and local time. The range is -12 to +12 hours. The default is 0 hours. This value is set with "CLOCK TIMEZONE" on page 333.
Daylight Savings Time (DST)	The status of the daylight savings time setting. The status can be enabled or disabled. This value is set with "CLOCK TIMEZONE" on page 333.

Example

The following example displays the settings of the SNTP client:

```
awplus# show ntp associations
```

SHOW NTP STATUS

Syntax

show ntp status

Parameters
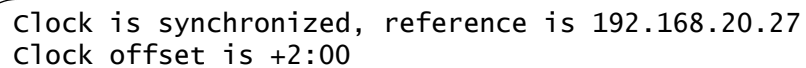
None

Mode

Privileged Exec mode

Description

Use this command to display the status of an NTP or SNTP server assigned to the switch. The display states whether or not the switch has synchronized its time with an NTP or SNTP server. An example of the display is shown in Figure 75.

```
Clock is synchronized, reference is 192.168.20.27
Clock offset is +2:00
```

Figure 75. SHOW NTP STATUS Command

The IP address above is the address of the NTP or SNTP server specified with the NTP PEER command. See "NTP PEER" on page 336. The clock offset is configured with the CLOCK TIMEZONE command. See "CLOCK TIMEZONE" on page 333.

Example

The following example displays the status of the NTP or SNTP server assigned to the switch:

awplus# show ntp status

341

Chapter 17

MAC Address Table

This chapter discusses the following topics:

Overview

The MAC address table stores the MAC addresses of all the network devices that are connected to the switch's ports. Each entry in the table consists of a MAC address, a port number where an address was learned by the switch, and an ID number of a VLAN where a port is a member.

The switch learns the MAC addresses of the network devices by examining the source addresses in the packets as they arrive on the ports. When the switch receives a packet that has a source address that is not in the table, it adds the address, along with the port number where the packet was received and the ID number of the VLAN where the port is a member. The result is a table that contains the MAC addresses of all the network devices that are connected to the switch's ports.

The purpose of the table is to allow the switch to forward packets more efficiently. When a packet arrives on a port, the switch examines the destination address in the packet and refers to its MAC address table to determine the port where the destination node of that address is connected. It then forwards the packet to that port and on to the network device.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all its ports, excluding the port where the packet was received. If the ports are grouped into virtual LANs, the switch floods the packet only to those ports that belong to the same VLAN from which the packet originated. This prevents packets from being forwarded to inappropriate LAN segments and increases network security. When the destination node responds, the switch adds the node's MAC address and port number to the MAC address table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Because both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This, too, increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

MAC addresses learned by the switch are referred to as dynamic addresses. Dynamic MAC addresses are not stored indefinitely in the MAC address table. They are automatically deleted when they are inactive. A MAC address is considered inactive if the switch does not receive any frames from the network device after a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

344

The period of time the switch waits before purging inactive dynamic MAC addresses is called the aging time. This value is adjustable on the switch. The default value is 300 seconds (5 minutes).

You can also enter addresses manually into the table. These addresses are referred to as static addresses. Static MAC addresses remain in the table indefinitely and are never deleted, even when the network devices are inactive. Static MAC addresses are useful for addresses that the switch might not learn through its normal learning process or for addresses that you want the switch to retain, even when the end nodes are inactive.

Adding Static MAC Addresses

The command for adding static unicast MAC addresses to the switch is MAC ADDRESS-TABLE STATIC in the Global Configuration mode. Here is the format of the command:

```
mac address-table static macaddress forward|discard
interface port [vlan vlan-name|vid]
```

Here are the variables of the command:

❑ *macaddress* - Use this variable to specify the unicast or multicast MAC address you want to add to the table. You can add only one address at a time. In the command, the address must be specified in either one of the following formats:

xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

❑ forward|discard - Use these variables to specify whether the port is to forward or discard packets that have the designated source MAC address.

❑ *port* - Use this variable to specify the port to which the end node of an address is connected. You can specify just one port.

❑ *vlan-name* or *VID* - Use this variable to specify the name or the ID number of the VLAN of the port of the address. This information is optional in the command.

This example adds the static MAC address 00:1B:75:62:10:84 to port 12 in the Default VLAN. The port forwards the packets of the designated network device:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 00:1b:75:62:10:84
forward interface port1.0.12 vlan 1
```

This example adds the static MAC address 00:A2:BC:34:D3:67 to port 11 in the VLAN with the ID 4. The port forwards the packets of the designated network device:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 00:a2:bc:34:d3:67
forward interface port1.0.11 vlan 4
```

This example adds the static MAC address 00:A0:D2:18:1A:11 to port 7. The port discards the packets of the designated network device:

346

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 00:a0:d2:18:1a:11
discard interface port1.0.7
```

Deleting MAC Addresses

To delete MAC addresses from the switch, use the CLEAR MAC ADDRESS-TABLE command in the Privileged Exec mode. The format of the command is:

```
clear mac address-table dynamic|static [address
macaddress]|[interface port]|[vlan vid]
```

Here are the variables:

- ❒ dynamic - This variable lets you delete dynamic addresses.
- ❒ static - This parameter lets you delete static addresses.
- ❒ address - You can use this parameter to delete specific addresses. You can delete just one address at a time. In the command, the address must be specified in either one of the following formats:

  xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

- ❒ interface - You can use this parameter to delete all of the static or dynamic addresses on a particular port. You can specify more than one port at a time.
- ❒ vlan - You can use this parameter to delete all of the static or dynamic addresses on the ports of a particular VLAN. You can specify just one VID at a time.

This example of the command deletes all of the dynamic addresses from the table:

```
awplus> enable
awplus# clear mac address-table dynamic
```

This example deletes all of the static addresses:

```
awplus> enable
awplus# clear mac address-table static
```

This example deletes a single dynamic address:

```
awplus> enable
awplus# clear mac address-table dynamic address
00:12:a3:68:79:b2
```

This example deletes a single static address:

```
awplus> enable
awplus# clear mac address-table static address
00:12:a3:d4:67:da
```

This example deletes all of the dynamic addresses learned on port 20:

```
awplus> enable
awplus# clear mac address-table dynamic interface port1.0.20
```

This example deletes all of the static addresses added to ports 2 to 5:

```
awplus> enable
awplus# clear mac address-table static interface port1.0.2-
port1.0.5
```

This example deletes all of the dynamic addresses learned on the ports of the VLAN with the VID 82:

```
awplus> enable
awplus# clear mac address-table dynamic vlan 82
```

This example deletes all of the static addresses added to the ports of the VLAN with the VID 18:

```
awplus> enable
awplus# clear mac address-table static vlan 18
```

Setting the Aging Timer

The aging timer defines the length of time that inactive dynamic MAC addresses remain in the table before they are deleted by the switch. The switch deletes inactive addresses to insure that the table contains only active and current addresses.

The aging timer does not apply to static addresses because static addresses are not deleted by the switch, even when the network devices are inactive.

To set the aging timer, use the MAC ADDRESS-TABLE AGEING-TIME command in the Global Configuration mode. Here is the format of the command:

```
mac address-table ageing-time value|none
```

The aging-time is expressed in seconds and has a range of 10 to 1000000 seconds. The default is 300 seconds (5 minutes). The value none disables the aging timer so that inactive MAC addresses are never deleted from the table.

To view the current setting for the MAC address aging timer, refer to "Displaying the MAC Address Table" on page 351.

This example sets the aging timer to 800 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table ageing-time 800
```

Displaying the MAC Address Table

To view the aging time or the MAC address table, use the SHOW MAC ADDRESS-TABLE command in the Privileged Exec mode. Here is its format:

```
show mac address-table [interface port]|[vlan vid]
```

An example of the table is shown in Figure 76.

```
Aging Interval: 300 second(s)

Switch Forwarding Database

--------------------------------------------------------------
VLAN    Port        MAC             Fwd
--------------------------------------------------------------
1       1.0.5       0011.2495.53f8  forward     dynamic
1       1.0.5       0023.6c90.08b9  forward     dynamic
1       1.0.5       0024.36a0.1551  forward     dynamic
1       1.0.5       0025.00d7.8908  forward     dynamic
1       1.0.5       0050.50de.ad01  forward     dynamic


.

.

.
--------------------------------------------------------------

Total Number of MAC Addresses: 121

Multicast Switch Forwarding Database
Total Number of MCAST MAC FDB Addresses: 1

----------------------------------------------------------------------
VLAN        MAC                     Port Maps (U:Untagged T:Tagged)
----------------------------------------------------------------------
1       01:00:51:00:00:01   Static  U:18-24
                                    T:
```

Figure 76. SHOW MAC ADDRESS-TABLE Command

The columns in the window are described in "SHOW MAC ADDRESS-TABLE" on page 362.

This example of the command displays the entire MAC address table:

```
awplus# show mac address-table
```

This example displays the MAC addresses learned on port 2:

```
awplus# show mac address-table interface port1.0.2
```

This example displays the addresses learned on the ports in a VLAN with the VID 8:

```
awplus# show mac address-table vlan 8
```

Chapter 18
MAC Address Table Commands

The MAC address table commands are summarized in Table 33.

Table 33. MAC Address Table Commands

Command	Mode	Description
"CLEAR MAC ADDRESS-TABLE" on page 354	Privileged Exec	Deletes MAC addresses from the MAC address table.
"MAC ADDRESS-TABLE AGEING-TIME" on page 356	Global Configuration	Sets the aging timer, which is used by the switch to identify inactive dynamic MAC addresses for deletion from the table.
"MAC ADDRESS-TABLE STATIC" on page 358	Global Configuration	Adds static unicast MAC addresses to the table.
"NO MAC ADDRESS-TABLE STATIC" on page 360	Global Configuration	Deletes static unicast MAC addresses from the table.
"SHOW MAC ADDRESS-TABLE" on page 362	Privileged Exec	Displays the MAC address table and the aging timer.

CLEAR MAC ADDRESS-TABLE

Syntax

```
clear mac address-table dynamic|static [address
macaddress]|[interface port]|[vlan vid]
```

Parameters

dynamic
> Deletes dynamic MAC addresses.

static
> Deletes static addresses.

address
> Deletes a specific address.

macaddress
> Specifies the address to be deleted. The address must be specified in either one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

interface
> Deletes MAC addresses learned on a specific port.

port
> Specifies the port the MAC addresses to be deleted was learned on. You can specify more than one port.

vlan
> Deletes MAC addresses learned on a specific VLAN.

vid
> Specifies the VID of the VLAN the MAC addresses to be deleted was learned on. You can specify just one VID.

Mode

Privileged Exec mode

Description

Use this command to delete addresses from the MAC address table.

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 362.

Examples

This example deletes all of the dynamic addresses from the table:

```
awplus> enable
awplus# clear mac address-table dynamic
```

This example deletes all of the static addresses:

```
awplus> enable
awplus# clear mac address-table static
```

This example deletes a single dynamic address:

```
awplus> enable
awplus# clear mac address-table dynamic address
00:12:a3:34:8b:32
```

This example deletes a single static address:

```
awplus> enable
awplus# clear mac address-table static address
00:12:a3:d4:67:da
```

This example deletes all of the dynamic addresses learned on ports 17 to 20:

```
awplus> enable
awplus# clear mac address-table dynamic interface port1.0.17-
port1.0.20
```

This example deletes all of the static addresses added to port 19:

```
awplus> enable
awplus# clear mac address-table static interface port1.0.19
```

This example deletes all of the dynamic addresses learned on the ports of the VLAN with the VID 12:

```
awplus> enable
awplus# clear mac address-table dynamic vlan 12
```

This example deletes all of the static addresses added to the ports of the VLAN with the VID 56:

```
awplus> enable
awplus# clear mac address-table static vlan 56
```

355

MAC ADDRESS-TABLE AGEING-TIME

Syntax

```
mac address-table ageing-time value|none
```

Parameter

ageing-time
> Specifies the aging timer in seconds for the MAC address table. The range is 10 to 1000000 seconds. The default is 300 seconds (5 minutes).

Mode

Global Configuration mode

Description

Use this command to set the aging timer. The aging timer is used by the switch to delete inactive dynamic MAC addresses from the MAC address table, to prevent the table from becoming full of inactive addresses. An address is considered inactive if no packets are sent to or received from the corresponding node for the duration of the timer.

Setting the aging timer to none disables the timer. No dynamic MAC addresses are aged out, and the table stops learning new addresses after reaching its maximum capacity.

To return the aging timer to its default value, use the NO form of this command.

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 362.

Examples

This example sets the aging timer to 500 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table ageing-time 500
```

This example disables the aging timer so that the switch does not delete inactive dynamic MAC addresses from the table:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table ageing-time none
```

This example returns the aging timer to its default setting of 300 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

MAC ADDRESS-TABLE STATIC

Syntax

```
mac address-table static macaddress forward|discard
interface port [vlan vlan-name|vid]
```

Parameters

macaddress

Specifies the static unicast address you want to add to the switch's MAC address table. The address must be specified in either one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

forward

Forwards packets containing the designated source MAC address.

discard

Discards packets containing the designated source MAC address.

port

Specifies the port(s) where the MAC address is to be assigned. A unicast MAC address can be added to only one port.

vlan-name

Specifies the name of the VLAN where the node designated by the MAC address is a member.

vid

Specifies the ID number of the VLAN where the node designated by the MAC address is a member. This parameter is optional.

Mode

Global Configuration mode

Description

Use this command to add static unicast MAC addresses to the switch's MAC address table. A static MAC address is never timed out from the MAC address table, even when the end node is inactive. You can add just one static MAC address at a time with this command.

The FORWARD and DISCARD parameters are used to specify whether the switch is to forward or discard packets containing the specified source MAC address.

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 362

Examples

This example adds the static MAC address 44:c3:22:17:62:a4 to port 4 in the Production VLAN. The port forwards the packets from the specified node:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 44:c3:22:17:62:a4
forward interface port1.0.4 vlan Production
```

This example adds the static MAC address 00:a0:d2:18:1d:11 to port 7 in the Default_VLAN, which has the VID 1. The port discards the packets from the specified node:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 00:a0:d2:18:1a:11
discard interface port1.0.7 vlan 1
```

This example adds the static MAC address 78:1a:45:c2:22:32 to port 15 in the Marketing VLAN. The port forwards the packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 78:1a:45:c2:22:32
forward interface port1.0.15 vlan Marketing
```

NO MAC ADDRESS-TABLE STATIC

Syntax

```
no mac address-table static macaddress forward|discard
interface port [vlan vlan-name|vid]
```

Parameters

macaddress

Specifies the static unicast address you want to delete from the switch's MAC address table. The address must be specified in either one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

forward

Forwards packets containing the designated source MAC address.

discard

Discards packets containing the designated source MAC address.

port

Specifies the port(s) where the MAC address is assigned.

vlan-name

Specifies the name of the VLAN where the node of the MAC address is a member. This parameter is optional.

vid

Specifies the ID number of the VLAN where the node of the MAC address is a member. You can omit this parameter when removing addresses from the Default_VLAN.

Mode

Global Configuration mode

Description

Use this command to delete dynamic or static unicast addresses from the switch's MAC address table. This command performs the same function as "CLEAR MAC ADDRESS-TABLE" on page 354.

Note
You cannot delete the switch's MAC address, an STP BPDU MAC address, or a broadcast address from the table.

360

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 362

Examples

This example deletes the MAC address 00:A0:D2:18:1A:11 from port 12 in the Default_VLAN, which has the VID 1. The port is forwarding packets of the owner of the address:

```
awplus> enable
awplus# configure terminal
awplus(config)# no mac address-table static
00:a0:d2:18:1a:11 forward interface port1.0.12 vlan 1
```

This example deletes the MAC address 86:24:3c:79:52:32 from port 16 in the Sales VLAN. The port is discarding packets of the owner of the address:

```
awplus> enable
awplus# configure terminal
awplus(config)# no mac address-table static
86:24:3c:79:52:32 discard interface port1.0.16 vlan Sales
```

SHOW MAC ADDRESS-TABLE

Syntax

```
show mac address-table begin|exclude|include [interface
port]|[vlan vid]
```

Parameters

begin

> Specifies the first line that matches the MAC address is displayed. The address must be specified in either one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

exclude

> Indicates the specified MAC address is excluded from the display. The address must be specified in either one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

include

> Indicates the specified MAC address is included in the display. The address must be specified in either one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

port

> Specifies a port. You may specify more than one port.

vid

> Specifies a VID. You may specify one VID.

Modes

Privileged Exec mode

Description

Use this command to display the aging timer and the unicast and multicast MAC addresses the switch has stored in the table. You may view all of the addresses in the table or only the addresses learned on a particular port or VLAN.

In addition, the software supports a GREP feature which allows you to specify a MAC address that is displayed or a MAC address that is not displayed by this command. You can also display MAC addresses that begin with a specified value.

An example of the table is shown in Figure 77.

```
Aging Interval: 300 second(s)

Switch Forwarding Database

--------------------------------------------------------------
VLAN    Port        MAC               Fwd
--------------------------------------------------------------
1       1.0.1     00a0.d218.1ac8    Forward    Dynamic
1       1.0.2     00a0.c416.3b80    Forward    Dynamic
1       1.0.3     00a0.12c2.10c6    Forward    Dynamic
1       1.0.4     00a0.c209.10d8    Forward    Dynamic
1       1.0.4     00a0.3343.a187    Forward    Dynamic
1       1.0.4     00a0.12a7.1468    Forward    Dynamic
.

.

.
--------------------------------------------------------------
Total Number of MAC Addresses: 121

Multicast Switch Forwarding Database
Total Number of MCAST MAC FDB Addresses: 1

-----------------------------------------------------------------------
VLAN          MAC                      Port Maps (U:Untagged T:Tagged)
-----------------------------------------------------------------------
1       01:00:51:00:00:01    Static    U:18-24
                                       T:
```

Figure 77. SHOW MAC ADDRESS-TABLE Command

The Aging Interval field at the top of the table displays the aging timer of the MAC address table.

The Switch Forwarding Database displays the static and dynamic unicast MAC addresses the switch has stored in the table. The first address is the MAC address of the switch. The columns are defined in Table 34.

Table 34. SHOW MAC ADDRESS-TABLE Command - Unicast Addresses

Parameter	Description
VLAN	The ID number of the VLAN where the port is an untagged member.
Port	The port where the address was learned or assigned. The MAC address with port 0 is the address of the switch.
MAC	The dynamic or static unicast MAC address learned on or assigned to the port.

Table 34. SHOW MAC ADDRESS-TABLE Command - Unicast Addresses

Parameter	Description
Fwd	The status of the address. MAC addresses have the status of Forward, meaning that they are used by the switch to forward packets.
(unlabeled)	The type of address: static or dynamic.

The Multicast Switch Forwarding Database contains the multicast addresses. The columns are defined in this table.

Table 35. SHOW MAC ADDRESS-TABLE Command - Multicast Addresses

Parameter	Description
VLAN	The ID number of the VLAN where the port is an untagged member.
MAC	The multicast MAC address.
(unlabeled)	The type of the address: static or dynamic.
Port Maps	The tagged and untagged ports on the switch that are members of the multicast group. This column is useful in determining which ports belong to different groups.

Examples

This example displays the entire MAC address table:

```
awplus# show mac address-table
```

This example displays the MAC addresses learned on ports 1 through 4:

```
awplus# show mac address-table interface port1.0.1-port1.0.4
```

This example displays the addresses learned on the ports in a VLAN with a VID of 22:

```
awplus# show mac address-table vlan 22
```

This example displays the MAC addresses that include a value of "90:08:B9:"

```
awplus# show mac address-table include 90:08:B9
```

Chapter 19
Enhanced Stacking

This chapter discusses the following topics:

Overview

Enhanced stacking is a management tool that allows you to manage different AT-9000 Switches from one management session. With enhanced stacking you can start a management session on one switch and then redirect the session to any of the other switches in the stack, without having to start a new session.

It is important to understand that enhanced stacking is simply a management tool. The switches of an enhanced stack continue to function as stand-alone devices. As such, the switches operate independently of each other and must be configured individually. For a description of how the feature is used, refer to "Managing the Member Switches of an Enhanced Stack" on page 374.

Note
Enhanced stacking is *only* supported on standalone switches. A standalone switch is defined as a switch with a Device ID set to 0.

Command and Member Switches

An enhanced stack must have one command switch. This switch is your management access point to the other switches in a stack. To manage the switches of a stack, you start a local or remote management session on the command switch and then redirect the session, as needed, to the other switches.

The other switches in the stack are known as member switches. They can be managed either through the command switch with enhanced stacking or from local or remote management sessions.

Common VLAN

❒ The switches of an enhanced stack do not have to be connected together with a common VLAN. The command switch uses this VLAN to send out broadcast packets to search for the switches in the stack. The VLAN also carries your configuration commands to the switches. Here are several things to keep in mind when planning the common VLAN of an enhanced stack:

❒ The common VLAN can have any valid VLAN name and VLAN identifier (VID).

❒ A member switch can be connected indirectly to the command switch through other switches, so long as there is an uninterrupted path of the common VLAN to the command switch.

❒ The Default_VLAN can be used as the common VLAN.

❒ The common VLAN of the enhanced stack does not have to be dedicated solely to that feature. It can be used like any other VLAN.

❐ A member switch can be any distance from the command switch, so long as the distance adheres to Ethernet cabling standards.

For background information on port-based and tagged virtual LANs, refer to Chapter 47, "Port-based and Tagged VLANs" on page 717.

Guidelines

Here are the enhanced stacking guidelines for the AT-9000 Switch:

❐ A stack can have up to 24 AT-9000 Switches.

❐ The switches of an enhanced stack must be connected together with a common port-based or tagged VLAN.

❐ The common VLAN does not require the same VID on all of the switches.

❐ You can use tagged or untagged twisted pair or fiber optic ports of the common VLAN to connect the switches together.

❐ A member switch does not have to be connected directly to the command switch. It can be connected indirectly through other switches, so long as there is an uninterrupted path of the common VLAN to the command switch.

❐ There are not any distance limitations between the command switch and the member switches of a stack, other than those dictated by the Ethernet cabling standards.

❐ The command switch is not required to be assigned a management IP address. The member switches also do not require IP addresses.

❐ You can create more than one enhanced stack in a network by assigning switches to different common VLANs.

❐ The enhanced stacking feature on the AT-9000 Switch is not compatible with the same feature on other Allied Telesis switches, such as the AT-8400, AT-8500, and AT-9400 Series switches.

❐ Remote Telnet, SSH, or web browser management of an enhanced stack must be conducted through the subnet of the common VLAN. The remote management workstations must be members of that subnet or have access to it through routers or other Layer 3 devices.

❐ The IP address 172.16.16.16 is reserved for the enhanced stacking feature. It must not be assigned to any device on your network.

General Steps

Here are the general steps to implementing the enhanced stacking feature on the switches:

1. Select an AT-9000 Switch to act as the command switch of the stack. This can be any AT-9000 Switch.

2. On the switch chosen to be the command switch, activate enhanced stacking and change its stacking status to command switch. The commands are ESTACK RUN and ESTACK COMMAND-SWITCH, both in the Global Configuration mode.

3. On the member switches, activate enhanced stacking. You do not have to set the enhanced stacking mode on the member switch because the member mode is the default setting.

4. Create a common port-based or tagged VLAN on the command and member switches. This step is not necessary if you are using the Default_VLAN (VID 1) as the common VLAN.

5. Optionally, assign the command switch a management IP address in the common VLAN.

6. If you plan to remotely manage the stack from management workstations that are not members of the same subnet as the switch, assign the command switch a default gateway that defines the first hop to reaching the subnet of the workstations.

   Since an enhanced stack is managed through the command switch, only that switch must have a default gateway, and only if the remote management workstations are not members of the same subnet as the common VLAN of the stack.

7. Connect the devices together using twisted pair or fiber optic ports of the common VLAN.

Configuring the Command Switch

Here is an example on how to configure the switch as the command switch of the enhanced stack. The example creates a common VLAN and assigns it a management IP address. Here are the specifications for this command switch:

- ❑ Common VLAN name: Tech_Support
- ❑ VID: 12
- ❑ Untagged VLAN ports: 18 to 22
- ❑ Management IP address and subnet mask: 149.22.88.5 and 255.255.255.0
- ❑ Default gateway: 149.22.88.27

(A default gateway is optional, but including it allows you to manage the switch and the enhanced stack from remote workstations that are not in the same subnet as the command switch.)

1. This step creates the common VLAN.

`awplus> enable`	Enter the Privileged Exec mode from the User Exec mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# vlan database`	From the Global Configuration mode, enter the VLAN Interface mode.
`awplus(config-vlan)# vlan 12 name Tech_Support`	Create the Tech_Support VLAN and assign it the VID 12.
`awplus(config-vlan)# exit`	Return to the Global Configuration mode.
`awplus(config)# interface port1.0.18-port1.0.22`	Enter the Port Interface mode for ports 18 to 22.
`awplus(config-if)# switchport mode access`	Designate the ports as untagged ports.
`awplus(config-if)# switchport access vlan 12`	Add the ports to the Tech_Support VLAN.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan 12`	Verify the new VLAN.

369

2. After creating the common VLAN on the switch, assign it the management IP address and default gateway:

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface vlan12`	From the Global Configuration mode, enter the VLAN Interface mode for the Tech_Support VLAN.
`awplus(config-if)# ip address 149.22.88.5/24`	Assign the VLAN the management IP address, 149.22.88.5 and the subnet mask, 255.255.255.0.
`awplus(config-if)# exit`	Return to the Global Configuration mode.
`awplus(config)# ip route 0.0.0.0/0 149.22.88.27`	Assign the switch the default gateway 149.22.88.27.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show ip interface`	Confirm the IP address.
`awplus# show ip route`	Confirm the default route.

3. Use the ESTACK RUN command in the Global Configuration mode to activate enhanced stacking and the ESTACK COMMAND-SWITCH command to set the enhanced stacking mode of the switch to command.

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# estack run`	Activate enhanced stacking on the switch.
`awplus(config)# estack command-switch`	Assign the switch the enhanced stacking status of command switch.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show estack`	Confirm the stack mode of the switch.

4. To save the configuration, enter the WRITE command in the Privileged Executive mode.

| awplus# write | Save the configuration. |

Configuring a Member Switch

This example shows you how to configure the switch as a member switch of an enhanced stack. It configures the switch to be part of the same enhanced stack with the same common VLAN as the command switch in the previous example. Here are the specifications for the member switch:

❒ Common VLAN name: Tech_Support

❒ VID: 12

❒ Untagged VLAN ports: 4 and 5

1. This step creates the common VLAN.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# vlan database`	Enter the VLAN Interface mode.
`awplus(config-vlan)# vlan 12 name Tech_Support`	Create the Tech_Support VLAN and assign it the VID 12.
`awplus(config-vlan)# exit`	Return to the Global Configuration mode.
`awplus(config)# interface port1.0.4-port1.0.5`	Enter the Port Interface mode for ports 4 to 5.
`awplus(config-if)# switchport mode access`	Designate the ports as untagged ports.
`awplus(config-if)# switchport access vlan 12`	Add ports 4 and 5 to the Tech_Support VLAN.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan 12`	Verify the new VLAN.

2. Use the ESTACK RUN command in the Global Configuration mode to activate enhanced stacking on the switch. It is not necessary to set the switch to the member mode because that is the default setting.

`awplus# configure terminal`	Enter the Global Configuration mode.

`awplus(config)# estack run`	Activate enhanced stacking on the switch.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show estack`	Confirm the stack mode of the switch.

3. To save the configuration, enter the WRITE command in the Privileged Executive mode.

`awplus# write`	Save the configuration.

4. Connect the switches together using ports of the common VLAN.

Managing the Member Switches of an Enhanced Stack

Here are the steps on how to manage the member switches of an enhanced stack.

1. Start a local or remote management session on the command switch of the enhanced stack. After logging on, you can view and configure the settings of just the command switch.

2. To manage a member switch in the enhanced stack, enter the SHOW ESTACK REMOTELIST command in the Privileged Exec mode.

   ```
   awplus> enable
   awplus# show estack remotelist
   ```

   This command displays all of the member switches in the stack. It does not display any command switches, including the command switch on which you started the management session. An example is shown here.

```
numOfNodes 2
Num  Mac Address        Name         Mode    Version        Model
---------------------------------------------------------------------
01   eccd.6d4d.6dd5     dutC         Member  AWPLUS v2.1.8.0  AT-9000/28
02   eccd.6d4d.6dd0     dutB         Member  AWPLUS v2.1.8.0  AT-9000/52
```

Figure 78. SHOW ESTACK REMOTELIST Command

3. Use the RCOMMAND command in the Global Configuration mode to redirect the management session from the command switch to one of the member switches in the list. The format of the command is shown here:

   rcommand *switch_id*

   For example, to manage the dutB switch in the list, you would enter this command:

   ```
   awplus# configure terminal
   awplus(config)# rcommand 2
   ```

   You can manage just one member switch at a time.

4. When prompted, enter the login name and password of a manager account on the member switch you are accessing. Once you have logged on, the command prompt for the member switch is displayed.

5. Configure or view the settings of the member switch, as needed.

374

6. When you are finished managing the member switch, enter the EXIT command from the User Exec mode or Privileged Exec mode to return the management session to the command switch.

7. To manage another member switch in the enhanced stack, repeat this procedure starting with Step 2.

8. To end the management session, return to the User Exec mode or Privileged Exec mode on the command switch and enter the EXIT command.

Changing the Enhanced Stacking Mode

If you want to change the enhanced stacking mode of a switch from command to member, all you have to do is enter the NO ESTACK COMMAND-SWITCH command in the Global Configuration mode, as shown here:

```
awplus> enable
awplus# configure terminal
awplus(config)# no estack command-switch
```

You can enter this command even if the enhanced stack is functional. Of course, once you have changed the mode on the switch to member from command, you cannot use the switch to manage the member switches in the stack.

Changing the switch from the member mode to the command mode can be more problematic, particularly if the enhanced stack is functional. This is because a member switch will not allow you to change its mode to the command mode if it is part of an active stack.

The easiest way to determine whether the switch is part of an active stack is to use the SHOW ESTACK command. An example of the command is shown here:

```
Enhanced Stacking mode        Member [1]
Management IP address         0.0.0.0
Mac address                   ECCD.6D4D.6DD5
Model Type                    AT-9000/28
Version Number                AWPLUS 2.1.8.0
```

Figure 79. SHOW ESTACK Command

If the brackets following "Member" are empty, the switch is not part of a stack, and you can use the ESTACK COMMMAND-SWITCH command in the Global Configuration mode to change its mode to command, as shown here:

```
awplus> enable
awplus# configure terminal
awplus(config)# estack command-switch
```

If there is a number in the brackets following "Member," the switch is a member of an active enhanced stack, and it will not let you change its mode. Here are the steps to follow in this situation:

1. On the command switch, disable enhanced stacking with the NO ESTACK RUN command.

2. On the member switch, change its mode from member to command with the ESTACK COMMAND-SWITCH command.

3. On the original command switch, restart enhanced stacking with the ESTACK RUN command and, if desired, reestablish its command mode with the ESTACK COMMAND-SWITCH command. (Disabling enhanced stacking changes the mode on a command switch from command to member.)

Uploading Boot Configuration Files from the Command Switch to Member Switches

You may use the enhanced stacking feature to transfer boot configuration files from the file system in the command switch of the enhanced stack to member switches. This allows you to use the command switch as a central storage device for the configuration files of the member switches in the stack and to distribute the files to the switches in the event you need to restore their configuration settings.

There are three situations where you are likely to find this feature useful:

❑ To restore the configuration to an existing member switch that has lost its configuration or that has the wrong configuration.

❑ To configure a replacement switch for a failed unit.

❑ To configure a new switch that is to have the same configuration as another switch.

There are several ways to use the feature. If the member switches share the same basic configuration, you could create a generic configuration file that contains most of the configuration settings for the switches in the stack and store the file on the command switch. To restore the configuration of a member switch, you could download this file to it from the command switch and afterwards, manually configure whatever other settings are needed for that specific member switch.

If the switches have different configurations, a generic configuration file may not be that useful. Instead, you could store each switch's unique configuration file on the command switch so that you can fully restore the configuration of any of the units.

To use the feature, you first have to store the configuration files of the member switches on the command switch. You can upload the files from the switches using TFTP or Zmodem and then download them into the file system of the command switch, again using TFTP or Zmodem.

The command for transferring configuration files is the UPLOAD CONFIG REMOTELIST command in the Global Configuration mode. The command itself does not have any parameters. Instead, it displays two prompts for the necessary information. The first prompt is shown here:

```
Enter the configuration file name ->
```

When you see this prompt, enter the name of the boot configuration file you want to transfer from the command switch to the member switches. You may specify just one filename, and the name must include the extension .cfg.

378

The second prompt is shown here:

```
Enter the list of switches ->
```

At the prompt, enter the enhanced stack numbers of the member switches to receive the file. You may upload a file to more than one member switch at a time by separating the numbers with commas. The numbers are viewed with the SHOW ESTACK REMOTELIST command.

There are certain things to know prior to using this feature:

- ❐ The transfer works from the command switch to the member switches. You may not use this feature to transfer configuration files from member switches to the command switch.

- ❐ You have to store the configuration files of the member switches in the file system of the command switch. To do that, you have to upload the files from the member switches using TFTP or Zmodem and then download them onto the command switch.

- ❐ Uploading a configuration file that contains the IP ADDRESS or IPV6 ADDRESS command to more than one switch may cause an IP address conflict in your network, in which multiple switches have the same IP address.

- ❐ A member switch has to be configured for enhanced stacking before the command switch can upload a configuration file to it. This means you have to activate enhanced stacking on it, and if the common VLAN of the enhanced stack is not the Default VLAN, you have to create the common VLAN on the switch.

- ❐ When a member switch receives a boot configuration file from the command switch, it stores the file in its file system as BOOT.CFG.

- ❐ You may upload any configuration file from the command switch, even the active boot configuration file.

Here are two examples of the feature. The first example restores a configuration file to an existing member switch of an enhanced stack. The example makes the following assumptions:

- ❐ Enhanced stacking is already activated on the member switch.

- ❐ The member switch already has the common VLAN that links the switches of the enhanced stack together.

- ❐ The name of its configuration file on the command switch is Eng12c.cfg.

- ❐ The member switch uses BOOT.CFG as its active boot configuration file, meaning it will not be necessary to change the name of the configuration file after is transferred to the member switch.

Here are the steps to perform on the command switch to upload the configuration file from its file system to the member switch:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# show estack remotelist`	Display the member switches of the enhanced stack with the SHOW ESTACK REMOTELIST command to learn the ID number of the switch to receive the configuration file.
`awplus# dir`	List the files in the file system of the command switch to confirm that it has the configuration file to upload to the member switch. In this example, the filename is Eng12c.cfg file.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# upload config remotelist`	Enter the UPLOAD CONFIG REMOTELIST command to begin the file transfer.
`Enter the configuration file name -> Eng12c.cfg`	At the prompt, enter the name of the configuration file the command switch is to upload to the member switch. The filename in this example is Eng12c.cfg.
`Enter the list of switches -> 3`	At the prompt, enter the enhanced stacking ID number of the member switch to receive the file. This number is learned with the SHOW ESTACK REMOTELIST command. The example assumes that the member switch has the ID number 3.
–	At this point, the command switch sends the file to the member switch, which stores it in its file system as BOOT.CFG.
`awplus(config_if)# reboot estack member 3`	Reboot the member switch so that it uses the new configuration file to set its parameters.

Here is another example of the feature. This example uploads a configuration file to a new switch in an enhanced stack, such as a replacement switch for a failed unit. This example is more complicated than the previous example because the stack is not using the Default VLAN as the common VLAN, and the new switch will not be using BOOT.CFG as the name of its active boot configuration file. The example makes the following assumptions:

❑ The common VLAN of the enhanced stack is called Network5a with the VID 25.

❑ The common VLAN will initially consist of just untagged port 1 on the new switch.

❑ The name of the boot configuration file to be downloaded to the new switch stored for the command switch is called SalesE4.cfg

❑ The name of the active boot configuration file on the new switch is to be actSalesE4.cfg

The first step is to create the common VLAN on the new switch. This is necessary because the enhanced stack is not using the Default VLAN as the common VLAN of the stack. To create the common VLAN and to activate enhanced stacking, perform these steps:

1. Start a local or remote management session on the new switch.

2. Create the common VLAN on the new switch with these commands.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# vlan database`	Enter the VLAN Interface mode.
`awplus(config-vlan)# vlan 25 name Network5a`	Create the Network5a VLAN and assign it the VID 25.
`awplus(config-vlan)# exit`	Return to the Global Configuration mode.
`awplus(config)# interface port1.0.1`	Enter the Port Interface mode for port 1.
`awplus(config-if)# switchport mode access`	Designate the port as an untagged port.
`awplus(config-if)# switchport access vlan 25`	Add port 1 to the Network5a VLAN.

381

`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan 12`	Verify the new VLAN.

3. Use the ESTACK RUN command in the Global Configuration mode to activate enhanced stacking on the switch. It is not necessary to set the switch to the member mode because that is the default setting.

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# estack run`	Activate enhanced stacking on the new switch.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show estack`	Confirm the stack mode of the switch.

4. To save the configuration, enter the WRITE command in the Privileged Executive mode.

`awplus# write`	Save the configuration.

5. Connect port 1 on the new switch to a port on another network device that is a member of the Network5A VLAN, such as the command switch.

Now that the replacement member switch is connected to the command switch through the common VLAN of the enhanced stack, you are ready to upload the SalesE4.cfg configuration file to it from the command switch with these steps:

1. Start a local or remote management session on the command switch of the enhanced stack.

2. Transfer the SalesE4.cfg configuration file from the command switch to the new member switch by performing these commands:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# show estack remotelist`	Display the SHOW ESTACK REMOTELIST command to learn the stack ID number of the replacement member switch.

`awplus# dir`	List the files in the file system of the command switch to confirm that it has the configuration file you want to upload to the member switch. In this example, the filename is Eng12c.cfg file.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# upload config remotelist`	Enter the UPLOAD CONFIG REMOTELIST command to begin the file transfer.
`Enter the configuration file name -> SalesE4.cfg`	At the prompt, enter the name of the configuration file the command switch is to upload to the member switch. In this example, the filename is SalesE4.cfg.
`Enter the list of switches -> 3`	At the prompt, enter the enhanced stacking ID number, learned with the SHOW ESTACK REMOTELIST command, of the member switch to receive the file. The example assumes that the ID number of the replacement member switch is 3.
`-`	At this point, the command switch sends the file to the member switch, which stores it in its file system as BOOT.CFG.

3. If the new member switch is to use BOOT.CFG as the name of its active boot configuration file, you complete the replacement procedure by resetting the switch to configure its parameters with the settings in the file. But because this example assumes that the name of the active boot configuration file has to be actSalesE4.cfg, you have to perform a few additional steps. You need to rename the BOOT.CFG file with the MOVE command and designate the file as the active boot configuration file with the BOOT CONFIG-FILE command. You can perform these tasks through enhanced stacking from the command switch, as shown in these steps:

`awplus(config)# exit`	On the command switch, return to the Privileged Exec mode.

383

`awplus# show estack remotelist`	Reconfirm the enhanced stacking ID number of the replacement member switch.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# rcommand 3`	Use the RCOMMAND command to start a remote management session on the replacement member switch. In this example the ID number of the switch is 3.
`Login: manager` `Password: ******`	Log on the replacement member switch.
`awplus> enable`	Enter the Privileged Exec mode.
`awplus(config)# move boot.cfg actSalesE4.cfg`	Rename the boot.cfg configuration file to actSalesE4.cfg.
`awplus(config)# boot config-file actSalesE4.cfg`	Designate the actSalesE4 file as the active boot configuration file on the switch.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# exit`	End your management session of the replacement member switch to return the session to the command switch.
`awplus(config)# reboot estack member 3`	From the command switch, reboot the replacement member switch so that it configures its parameters with the actSalesE4.cfg configuration file.

Uploading the Management Software from the Command Switch to Member Switches

You may use enhanced stacking to install new releases of the management software on the member switches from the command switch. After you update the command switch with the new management software, you can instruct it to upload the software to the member switches for you.

After you receive a new release of the management software and install it on the command switch, as explained in "Downloading New Management Software with TFTP" on page 491, you may use the UPLOAD IMAGE REMOTELIST command to upload the software to the member switches from the command switch. You may update specific member switches or all of the switches. The format of the command is shown here:

```
upload image remotelist
```

The command, located in the Global Configuration mode, does not have any parameters and displays this prompt:

```
Remote switches will reboot after load is complete...
Enter the list of switches ->
```

When you see this prompt, enter the enhanced stacking ID numbers of the member switches to receive the management software from the command switch. The numbers are viewed with the SHOW ESTACK REMOTELIST command in the Privileged Exec mode. You may update the management software on more than one member switch at a time. To specify more than one switch, separate the numbers with commas. To update all of the switches in the enhanced stack, enter ALL.

Here are the steps of the file transfer between the command switch and a member switch:

1. The command switch sends its management software to the member switch over the Ethernet link of the common VLAN that connects the switches of the enhanced stack.

2. After the member switch receives the entire file, it compares the version numbers of the new management software from the command switch and its current software.

3. If the version numbers are the same, the switch cancels the update and discards the file.

4. If the version numbers of the programs are different, the switch writes the new management software from the command switch into its flash memory. This phase may take up to one minute to complete.

5. After the file is written to flash memory, the member switch resets.

> ⚠️ **Caution**
>
> A member switch stops forwarding network traffic after it receives the management software from the command switch and begins writing it to flash memory. Some network traffic may be lost.

> ⚠️ **Caution**
>
> Do not power off a member switch while it is writing the software to flash memory.

Here in this example of the command, the command switch uploads its management software to two member switches that have the ID numbers, 5 and 6. The procedure assumes that the new management software is already installed on the command switch.

`awplus> enable`	Enter the Privileged Exec mode from the User Exec mode.
`awplus# show estack remotelist`	Display the enhanced stacking ID numbers of the member switches in the stack. You should perform this command even if you intend to update all of the member switches, to ensure that the command switch is aware of all of the member switches that comprise the stack.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# upload image remotelist`	Start the upload with the UPLOAD IMAGE REMOTELIST command.
`Remote switches will reboot after load is complete ...` `Enter the list of switches -> 5,6`	At the prompt, enter 5 and 6, the enhanced stacking ID numbers of the two member switches to be upgraded.

Disabling Enhanced Stacking

The command that disables enhanced stacking on a switch is the NO ESTACK RUN command in the Global Configuration mode, and the confirmation command is the SHOW ESTACK command in the Privileged Exec mode.

You may not use the NO ESTACK RUN command when you are managing a member switch through enhanced stacking. You may only use the command when you are managing a switch directly, from a local management session or a remote Telnet, SSH, or web browser session.

When you disable enhanced stacking on a command switch, you may not use the switch to manage the member switches of an enhanced stack. It should be noted that disabling enhanced stacking on a command switch returns the mode to the member switch mode. So if you reactivate enhanced stacking, the switch is a member switch, unless you change it again with the ESTACK COMMAND-STACK command.

Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no estack run
```

Chapter 20

Enhanced Stacking Commands

The enhanced stacking commands are summarized in Table 36.

Table 36. Enhanced Stacking Commands

Command	Mode	Description
"ESTACK COMMAND-SWITCH" on page 391	Global Configuration	Designates the switch as the command switch.
"ESTACK RUN" on page 392	Global Configuration	Activates enhanced stacking on the switch.
"NO ESTACK COMMAND-SWITCH" on page 393	Global Configuration	Returns the switch to the state of being a member switch.
"NO ESTACK RUN" on page 394	Global Configuration	Disables enhanced stacking on the switch.
"RCOMMAND" on page 395	Global Configuration	Redirects the management session to a different switch in the enhanced stack.
"REBOOT ESTACK MEMBER" on page 396	Global Configuration	Reboots member switches of an enhanced stack from the command switch.
"SHOW ESTACK" on page 398	Privileged Exec	Displays whether the switch is a command or member switch and whether enhanced stacking is enabled or disabled.
"SHOW ESTACK COMMAND-SWITCH" on page 400	Privileged Exec	Displays enhanced stacking information about the command switch from a member switch.
"SHOW ESTACK REMOTELIST" on page 401	Privileged Exec	Displays the switches of an enhanced stack.
"UPLOAD CONFIG REMOTELIST" on page 403	Global Configuration	Uploads boot configuration files from the file system in the command switch of an enhanced stack to the member switches.

Table 36. Enhanced Stacking Commands

Command	Mode	Description
"UPLOAD IMAGE REMOTELIST" on page 404	Global Configuration	Uploads the management software on the command switch of an enhanced stack to the member switches.

ESTACK COMMAND-SWITCH

Syntax

```
estack command-switch
```

Parameter

None

Mode

Global Configuration mode

Description

❐ Use this command to set the enhanced stacking mode on the switch to the command mode. This command has the following guidelines:

❐ Enhanced stacking must be activated on the switch. To activate enhanced stacking, refer to "ESTACK RUN" on page 392.

❐ A switch that is a member of an active enhanced stack cannot be changed to the command mode. You must first disable enhanced stacking on the current command switch in the stack.

❐ You cannot use this command on a switch accessed through enhanced stacking. This command can only be used from a local or remote management session of the switch.

Confirmation Command

"SHOW ESTACK" on page 398

Example

This example activates enhanced stacking on the switch and sets the stacking status to command mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# estack run
awplus(config)# estack command-switch
```

391

ESTACK RUN

Syntax

```
estack run
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to activate enhanced stacking on the switch.

Confirmation Command

"SHOW ESTACK" on page 398

Example

The following example activates enhanced stacking on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# estack run
```

NO ESTACK COMMAND-SWITCH

Syntax

```
no estack command-switch
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to return the enhanced stacking mode on the switch to member switch from command switch. This command has the following guidelines:

□ The default setting for the enhanced stacking mode on the switch is member. So you would only use this command if you set the mode to command mode and now want to return it to member mode.

□ Enhanced stacking must be activated on the switch for you to use the command. To activate enhanced stacking, refer to "ESTACK RUN" on page 392.

□ You cannot use this command on a switch accessed through enhanced stacking. This command can only be used from a local or remote management session of the switch.

To configure the switch as a command switch, refer to "ESTACK COMMAND-SWITCH" on page 391.

Confirmation Command

"SHOW ESTACK" on page 398

Example

This example returns the switch's stacking status to member switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no estack command-switch
```

NO ESTACK RUN

Syntax

```
no estack run
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to disable enhanced stacking on the switch. The switch cannot use enhanced stacking when the feature is disabled. If you disable enhanced stacking on the command switch, you cannot use that switch to manage the switches in the stack.

When you disable enhanced stacking on the command switch, its mode is reset to member mode. Consequently, you must set it back again to the command mode if you reactivate enhanced stacking.

Note
You should only use this command from a local or remote management session of the switch. You should not issue this command on a member switch that you accessed through enhanced stacking. Otherwise, your management session will be interrupted.

Confirmation Command

"SHOW ESTACK" on page 398

Example

This example deactivates enhanced stacking on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no estack run
```

RCOMMAND

Syntax

rcommand *switch_id*

Parameters

switch_id
> Specifies the ID number of a member switch you want to manage in the enhanced stack. This number is displayed with "SHOW ESTACK REMOTELIST" on page 401. You can enter only one ID number.

Mode

Global Configuration mode

Description

Use this command to redirect the management session from the command switch to a member switch in the enhanced stack. The member switch is identified by its ID number, displayed with "SHOW ESTACK REMOTELIST" on page 401. You can manage only one member switch at a time.

Note
You must perform this command from the command switch of the stack. This command will not work on a member switch.

Note
You should perform the SHOW ESTACK REMOTELIST command before this command.

When you are finished managing a member switch, use the EXIT command to return to the command switch.

Example

This example starts a management session on switch number 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# rcommand 12
```

REBOOT ESTACK MEMBER

Syntax

```
reboot estack member id_number | all
```

Parameters

id_number

Specifies the enhanced stack ID number of a switch. The number is displayed with "SHOW ESTACK REMOTELIST" on page 401. You may specify the ID number of only one switch.

all

Specifies all of the switches of the enhanced stack, except the command switch.

Mode

Global Configuration mode

Description

Use this command from the command stack of an enhanced switch to reboot member switches. You may reboot individual member switches or all of the member switches of a stack. You must perform "SHOW ESTACK REMOTELIST" on page 401 prior to this command to determine the ID numbers of the switches.

⚠️ **Caution**

A switch does not forward network traffic when it reboots and initializes its management software. Some network traffic may be lost. The reset can take from 10 seconds to two minutes, depending on the number and complexity of the commands in the active boot configuration file.

Note

Any configuration changes that are not saved to the active configuration file with the WRITE command are discarded when a switch reboots.

⚠️ **Caution**

This command does not display a confirmation prompt. A member switch resets as soon as you enter the command.

Examples

This example reboots a member switch that has the ID number 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# reboot estack member 3
```

This example reboots all of the member switches of the enhanced stack:

```
awplus> enable
awplus# configure terminal
awplus(config)# reboot estack member all
```

SHOW ESTACK

Syntax

```
show estack
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display whether enhanced stacking is enabled or disabled on the switch and whether the switch's mode is command or member. Figure 80 is an example of the information the command displays.

```
Enhanced Stacking mode          Member [1]
 MAC address                    00:15:77:cc:e2:42
 Model Type                     AT-9000/52
 Version Number                 AWPLUS 2.1.8.0
```

Figure 80. SHOW ESTACK Command

The fields are described in Table 37 on page 398.

Table 37. SHOW ESTACK Command

Parameter	Description
Enhanced Stacking mode	The status of enhanced stacking on the switch and the mode of the switch. The possible modes are: ❐ Command - Enhanced stacking is enabled on the switch, and the switch is set to the command mode.

Table 37. SHOW ESTACK Command (Continued)

Parameter	Description
Enhanced Stacking mode (Continued)	❒ Member [1] - Enhanced stacking is enabled on the switch, and the switch is set to the member mode. If there is a number in the brackets, the switch detected a command switch on the common VLAN of the enhanced stack. The number is the switch's stack ID number. If the brackets are empty, the switch did not detect a command switch on the common VLAN and so does not consider itself part of an enhanced stack. ❒ Disabled - Enhanced stacking is disabled on the switch.
MAC address	The switch's MAC address.
Model Type	The model name of the switch.
Version Number	The name and version number of the management software on the switch. The name of the management software for the AT-9000 Switch is displayed as AWPLUS, for AlliedWare Plus.

Example

The following example displays whether enhanced stacking is enabled or disabled on the switch and whether the switch's mode is command or member:

```
awplus> enable
awplus# show estack
```

399

SHOW ESTACK COMMAND-SWITCH

Syntax

show estack command-switch

Parameters

None

Mode

Privileged Exec mode

Description

Use this command on a member switch in an enhanced stack to display the enhanced stacking information about the command switch. This command is equivalent to issuing the SHOW ESTACK command on the command switch. Figure 81 is an example of the information the command displays.

```
Enhanced Stacking mode          Member [1]
Management IP address           0.0.0.0
Mac address                     ECCD.6D4D.6DD5
Model Type                      AT-9000/52
Version Number                  AWPLUS 2.1.8.0
```

Figure 81. SHOW ESTACK COMMAND-SWITCH Command

The fields are described in Table 37 on page 398.

Example

The following example displays the enhanced stacking information about the command switch:

```
awplus> enable
awplus# show estack command-switch
```

SHOW ESTACK REMOTELIST

Syntax

show estack remotelist [name] [series]

Parameters

name
　　　Sorts the list of switches by the host name.

series
　　　Sorts the list of switches by the model name.

Mode

Privileged Exec mode

Description

Use this command on the command switch to display the member switches of an enhanced stack. You may sort the names by MAC address, host name, or model series. The default is MAC address. An example is shown in Figure 82.

```
numOfNodes 2
Num  Mac Address        Name          Mode    Version         Model
------------------------------------------------------------------------
01   eccd.6d4d.6dd5     dutC          Member  AWPLUS v2.1.8.0  AT-9000/28
02   eccd.6d4d.6dd0     dutB          Member  AWPLUS v2.1.8.0  AT-9000/28SP
```

Figure 82. SHOW ESTACK REMOTELIST Command

The list does not include the command switch on which you entered the command.

Note
This command only works on the command switch of the stack. It does not work on member switches.

Examples

This example displays the member switches of an enhanced stack by MAC address:

```
awplus> enable
awplus# show estack remotelist
```

This example sorts the switches by host name:

```
awplus> enable
awplus# configure terminal
awplus(config)# show estack remotelist name
```

This example sorts the switches by model series:

```
awplus> enable
awplus# configure terminal
awplus(config)# show estack remotelist series
```

UPLOAD CONFIG REMOTELIST

Syntax

```
upload config remotelist
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to upload boot configuration files from the file system in the command switch of an enhanced stack to the member switches. The member switches store the files in their file systems as BOOT.CFG.

The command displays two prompts. The first prompt is shown here:

```
Enter the configuration file name ->
```

When you see this prompt, enter the name of the boot configuration file to transfer from the command switch to the member switches. You may specify only one filename, and the name must include the extension .cfg.

The second prompt is shown here:

```
Enter the list of switches ->
```

At this prompt, enter the enhanced stack numbers of the member switches to receive the file. If you are uploading a file to more than one switch, separate the numbers with commas. The numbers are viewed with the SHOW ESTACK REMOTELIST command.

Example

This example uploads the Sw12a.cfg configuration file from the file system of the command switch to a member switch that has the ID number 3. The member switch stores the file as BOOT.CFG in its file system:

```
awplus> enable
awplus# configure terminal
awplus(config)# upload config remotelist
Enter the configuration file name -> sw12a.cfg
Enter the list of switches -> 3
```

UPLOAD IMAGE REMOTELIST

Syntax

upload image remotelist

Parameters

None

Mode

Global Configuration mode

Description

Use this command to upload the management software on the command switch of an enhanced stack to the member switches. The command displays the following prompt:

Remote switches will reboot after load is complete...
Enter the list of switches ->

When you see this prompt, enter the enhanced stack numbers of the member switches to receive the management software from the command switch. You may update the management software on more than one member switch at a time. To specify more than one switch, separate the numbers with commas. To update all of the switches in the enhanced stack, enter ALL. The numbers are viewed with the SHOW ESTACK REMOTELIST command in the Privileged Exec mode.

Here are the steps of the file transfer between the command switch and a member switch:

1. The command switch sends its management software to the member switch over the Ethernet link of the common VLAN that connects the switches of the enhanced stack.

2. After the member switch has received the entire file, it compares the version numbers of the new management software from the command switch and its current software.

3. If the version numbers are the same, the switch cancels the update and discards the file.

4. If the version numbers are different, the member switch writes the file to its flash memory. This phase may take up to one minute to complete.

5. After the file is written to flash memory, the member switch resets.

> ⚠️ **Caution**
>
> The member switches stop forwarding network traffic after they receive the management software from the command switch and as they write the file to their flash memory. Some network traffic may be lost.

> ⚠️ **Caution**
>
> Do not power off the member switches while they are writing the software to their flash memory.

Example

This example uploads the management software on the command switch to two member switches that have the ID numbers 1 and 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# upload image remotelist
Remote switches will reboot after load is complete...
Enter the list of switches -> 1,5
...Uploading 13316011 bytes. Please wait...

Upload image to Member Switches complete. <120 sec.>
```

Chapter 21

Port Mirror

This chapter discusses the following topics:

407

Overview

The port mirror is a management tool that allows you to monitor the traffic on one or more ports on the switch. It works by copying the traffic from designated ports to another port where the traffic can be monitored with a network analyzer. The port mirror can be used to troubleshoot network problems or to investigate possible unauthorized network access. The performance and speed of the switch is not affected by the port mirror.

To use this feature, you must designate one or more source ports and the destination port. The source ports are the ports whose packets are to be mirrored and monitored. The destination port is the port where the packets from the source ports are copied and where the network analyzer is connected. There can be only one destination port on the switch.

Here are the guidelines for the port mirror:

- The switch supports only one port mirror.
- The port mirror can have just one destination port.
- The port mirror can have more than one source port. This allows you to monitor the traffic on multiple ports at the same time. For example, you might monitor the traffic on all the ports of a particular VLAN.
- You can mirror the ingress traffic, the egress traffic or both on the source ports.
- The destination port should not be a member of a static port trunk or an LACP trunk.

Creating the Port Mirror or Adding New Source Ports

The command to create the port mirror is the MIRROR INTERFACE command. You must perform this command from the Port Interface mode of the destination port of the port mirror. The command has this format:

```
mirror interface source_ports direction
receive|transmit|both
```

This example configures the port mirror to copy the ingress traffic on the source port 3 to the destination port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.3 direction
receive
```

The switch immediately begins to copy the monitored traffic from the source ports to the destination port as soon as you create the port mirror.

To add new source ports to the port mirror, return to the Port Interface mode of the destination port and enter the same command. For example, to monitor both the ingress and egress traffic on ports 11 and 12 to the destination port 5, you enter:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.11-port1.0.12
direction both
```

For reference information, refer to "MIRROR INTERFACE" on page 417.

Removing Source Ports or Deleting the Port Mirror

To remove source ports from the port mirror, enter the Port Interface mode of the destination port and issue the NO MIRROR INTERFACE command. Here is the format of the command:

```
no mirror interface source_ports
```

This example removes source port 2 from the port mirror. The destination port is port 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11
awplus(config-if)# no mirror interface port1.0.2
```

To stop port mirroring and return the destination port to normal network operations, remove all of the source ports from the port mirror. For example, if the source ports of the port mirror were ports 1 to 4, and the destination port was 18, you would enter these commands to stop the port mirror and reestablish normal network operations on the destination port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18
awplus(config-if)# no mirror interface port1.0.1-port1.0.4
```

For reference information, refer to "NO MIRROR INTERFACE" on page 419.

Combining the Port Mirror with Access Control Lists

You may combine the port mirror with an access control list to monitor a subset of the ingress traffic on a port. The access control list is used to specify the ingress traffic to be coped to the destination port of the port mirror. This feature only works on ingress packets because access control lists are only effective on those types of packets. You cannot use it to copy a subset of the egress packets on a port.

You first have to specify the destination port of the port mirror. The switch can have only one destination port. The command for specifying the destination port is the MIRROR command in the Port Interface mode. The mode in which to perform the command is the Port Interface mode of the port to be the destination port for the monitored traffic the access control list defines.

You then have to create the access control list and assign it to the port whose packets you want to monitor. When you create the access control list, you have to specify the copy-to-mirror action.

Here is an example of the feature. It assumes you want to monitor ports 14 and 15 for ingress packets that have the IP address 149.83.124.95 as their destination address. The traffic is to be copied to port 18, the destination port for the port mirror. The access control list is given the ID number 3008.

`awplus> enable`	Enter the Privileged Exec mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.18`	Enter the Port Interface mode for port 18, the destination port for the port mirror.
`awplus(config-if)# mirror`	Enter the MIRROR command to designate port 18 as the destination port for the copied packets.
`awplus(config-if)# exit`	Return to the Global Configuration mode.
`awplus(config)# access-list 3008 copy-to-mirror ip any 149.83.124.95/32`	Create the access control list. The source address is ANY and the destination address is 149.83.124.95.

`awplus(config)# interface port1.0.14,port1.0.15`	Enter the Port Interface modes for ports 14 and 15.
`awplus(config-if)# access-group 3008`	Assign the access control list to the ports.
`awplus(config-if)# end`	Return to the Privileged Exec mode.

`awplus# show mirror`
 	
`Mirror-To-Port Name: Port1.0.18`
	Use the SHOW MIRROR command to confirm that port 18 is the destination port of the port mirror.

`awplus# show access-list`
 	
`Hardware IP access-list 3008`
`    copy-to-mirror ip any 149.83.124.95 mask 255.255.255.255`
`Total number of access-list = 1`
	Use the SHOW ACCESS-LIST command to confirm the configuration of the access control list.

`awplus# show interface port1.0.14,port1.0.15 access-group`
 	
`Interface port1.0.14`
`    access-group 3008`
`Interface port1.0.15`
 	
`    access-group 3008`
	Use the SHOW INTERFACE ACCESS-GROUP command to confirm that the access control list is assigned to ports 14 and 15.

412

Displaying the Port Mirror

To display the port mirror, go to the Privileged Exec mode and enter the SHOW MIRROR command:

```
awplus# show mirror
```

In this example of the information, the port mirror is enabled, and the ingress and egress packets on ports 1 and 3, as well as the egress traffic on ports 11 to 13, are being copied to destination port 22.

Destination Port —————— Mirror Test Port Name: port1.0.22
Source Port —————— Mirror option: Enabled
Mirror direction: both
Destination Port —————— Monitored Port Name: port1.0.1
Mirror Test Port Name: port1.0.22
Source Port —————— Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.4
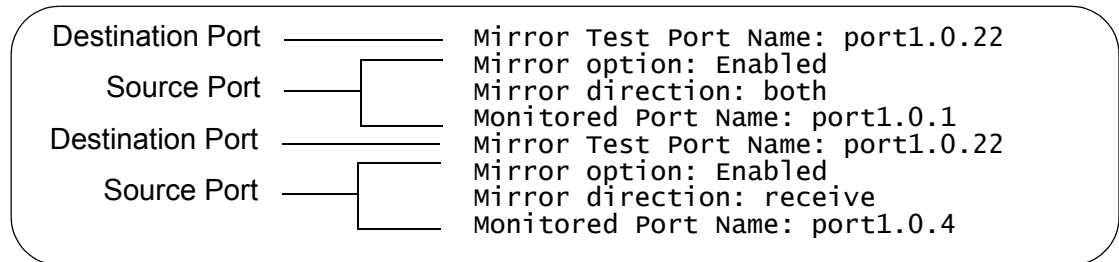
Figure 83. SHOW MIRROR Command

The fields are described in Table 39 on page 420.

If you are using the port mirror with access control lists to copy subsets of ingress packets on source ports, the SHOW MIRROR command displays only the destination port of the copied traffic. Here is an example.

```
Mirror-To-Port Name: port1.0.11
```

Figure 84. SHOW MIRROR Command and Access Control Lists

To view the access control lists and their port assignments, use "SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264, respectively.

414

Chapter 22
Port Mirror Commands

The port mirror commands are summarized in Table 38.

Table 38. Port Mirror Commands

Command	Mode	Description
"MIRROR" on page 416	Port Interface	Designates the destination port for access control lists that use the copy-to-mirror action.
"MIRROR INTERFACE" on page 417	Port Interface	Creates the port mirror and adds ports to the port mirror.
"NO MIRROR INTERFACE" on page 419	Port Interface	Removes source ports from the port mirror and deletes the port mirror.
"SHOW MIRROR" on page 420	Privileged Exec	Displays the destination port and source ports of the port mirror.

MIRROR

Syntax

```
mirror
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to designate the destination port for the copy-to-mirror action in access control lists. You can designate only one destination port.

Confirmation Command

"SHOW MIRROR" on page 420

Example

This example designates port 21 as the destination port for packets from the copy-to-mirror action of access control lists:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror
```

MIRROR INTERFACE

Syntax

```
mirror interface source_ports direction
receive/transmit/both
```

Parameters

source_ports
> Specifies a source port for the port mirror. You can specify more than one source port.

direction
> Specifies the traffic to be mirrored from a source port to the destination port. The options are:
>
> > *receive*: Copies the ingress packets on a source port.
> >
> > *transmit:* Copies the egress packets on a source port.
> >
> > *both:* Copies both the ingress and egress packets on a source port.

Mode

Port Interface mode

Description

Use this command to create the port mirror or to add ports to the port mirror. You must issue this command from the Port Interface mode of the destination port of the port mirror. The switch can have only one destination port.

Confirmation Command

"SHOW MIRROR" on page 420

Example

This example configures the port mirror to copy the ingress traffic on ports 3 and 4, the source ports, to port 5, the destination port. If port 5 is already acting as the destination port of the port mirror, the commands add ports 3 and 4 to the port mirror:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.3,port1.0.4
direction receive
```

418

NO MIRROR INTERFACE

Syntax

```
no mirror interface source_ports
```

Parameters

source_ports
> Specifies a source port of the port mirror. You can specify more than one source port at a time in the command.

Mode

Port Interface mode

Description

Use this command to remove source ports from the port mirror or to delete the port mirror. You should enter this command in the Port Interface mode of the destination port of the port mirror.

To delete the port mirror and return the destination port to normal operations, remove all of the source ports from the port mirror.

Confirmation Command

"SHOW MIRROR" on page 420

Example

These commands remove ports 7 and 8 from the port mirror. If these are the only source ports of the port mirror, the port mirror is deleted and the destination port, which in this example is port 11, resumes normal network operations:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11
awplus(config-if)# no mirror interface port1.0.7,port1.0.8
```

SHOW MIRROR

Syntax

```
show mirror
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the source and destination ports of the port mirror on the switch. An example is shown in Figure 85.
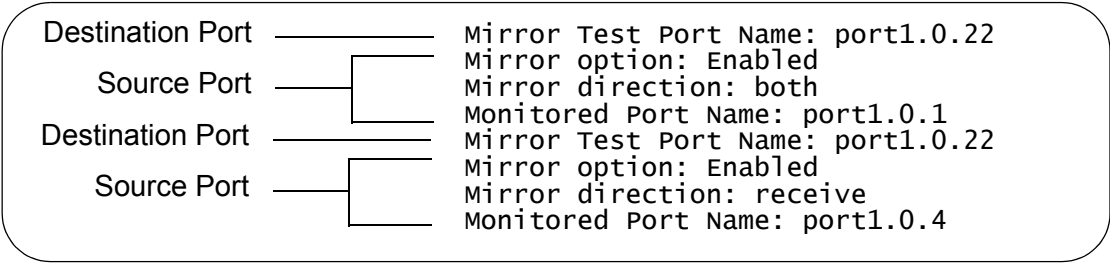
Figure 85. SHOW MIRROR Command

The fields are described in Table 39.

Table 39. SHOW MIRROR Command

Parameter	Description
Mirror Test Port Name	The destination port of the port mirror. The switch can have only one destination port.
Mirror option:	The status of the port mirror on the source port. This is always enabled.

Table 39. SHOW MIRROR Command (Continued)

Parameter	Description
Mirror direction	The packets to be mirrored to the destination port. The states are listed here: ❐ Receive - The ingress packets of the source port are mirrored to the destination port. ❐ Transmit - The egress packets of the source port are mirrored to the destination port. ❐ Both - Both the ingress and egress packets of the source port are mirrored to the destination port.
Monitored Port Name	A source port of the port mirror.

If you are using the port mirror with access control lists to copy subsets of ingress packets on source ports, the SHOW MIRROR command displays only the destination port of the copied traffic. Here is an example.

```
Mirror-To-Port Name: port1.0.11
```

Figure 86. SHOW MIRROR Command and Access Control Lists

To view the access control lists and their port assignments, use "SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264, respectively.

Example

The following example displays the source and destination ports of the port mirror on the switch:

awplus# show mirror

Chapter 23

Internet Group Management Protocol (IGMP) Snooping

This chapter discusses the following topics:

Overview

IGMP snooping allows the switch to control the flow of multicast packets from its ports. It enables the switch to forward packets of multicast groups to only ports that have host nodes that want to join the multicast groups.

IGMP is used by IPv4 routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node that wants to become a member of a multicast group responds to a query by sending a report. A report indicates that an end node wants to become a member of a multicast group. Nodes that join a multicast group are referred to as host nodes. After joining a multicast group, a host node must continue to periodically issue reports to remain a member.

After the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting the multicast packets only to router ports where host nodes are located.

There are three versions of IGMP— versions 1, 2, and 3. One of the differences between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In version 1, it stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames and removes it from the membership list of the multicast group.

In version 2, a host node exits from a multicast group by sending a *leave request*. After receiving a leave request from a host node, the router removes the node from the appropriate membership list. The router also stops sending multicast packets out the port to which the node is connected if it determines there are no further host nodes on the port.

Version 3 adds the ability to register multiple groups using a group list within a single packet.

The IGMP snooping feature on the switch supports all three versions of IGMP. The switch monitors the flow of queries from routers, and reports leave messages from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This

424

improves switch performance and network security by restricting the flow of multicast packets to only those switch ports that are connected to host nodes.

If the switch is not using IGMP snooping and receives multicast packets, it floods the packets out all its ports, except the port on which it received the packets. Such flooding of packets can negatively impact network performance.

The switch maintains its list of multicast groups through an adjustable timeout value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note
The default setting for IGMP snooping on the switch is enabled.

Understanding Multicast Traffic Settings

By default, IGMP snooping is disabled on the switch. As a result, this setting can impact multicast settings on a port. When you block egress or ingress multicast packets on a port and the switch is set to IGMP snooping disabled, the result is that *all* reports are suppressed on the specified ports except for reserved multicast addresses.

When you enable IGMP Snooping by executing the IP IGMP SNOOPING command, *all* unknown multicast traffic is unsuppressed and floods the switch ports except for IPv4 reserved addresses 224.0.0.1 through 224.0.0.255. To enable the suppression of unknown multicast traffic, see "Enabling the Suppression of Unknown Multicast Traffic".

For information about how to block egress and ingress multicast packets, see "SWITCHPORT BLOCK EGRESS-MULTICAST" on page 450 and "SWITCHPORT BLOCK INGRESS-MULTICAST" on page 451.

Enabling the Suppression of Unknown Multicast Traffic

IGMP snooping does not suppress all unknown multicast traffic except for IPv4 reserved addresses in the range of 224.0.0.1 to 224.0.0.255 by default. To suppress the flooding, use the NO IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST command. When you execute this command, all unknown multicast traffic is suppressed prior to a join message. Once a join message is accepted for the specified multicast destination, it is no longer considered an unknown destination and, therefore, no longer floods. For more information about this command, see "IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST" on page 438.

Host Node Topology

The switch has a host node topology setting. You use this setting to define whether there is more than one host node on each port on the switch. The switch refers to the topology to determine whether or not to continue transmitting multicast packets from ports that receive leave requests or where host nodes time out due to inactivity. The possible topology settings are:

❐ Single-host per port

❐ Multiple-hosts per port

Single-host Per Port

This is the appropriate setting when there is only one host node connected to each port on the switch. When this topology setting is enabled, the switch immediately stops sending multicast packets from ports on which host nodes have sent leave requests or have timed out. The switch responds by immediately ceasing the transmission of additional multicast packets out the ports.

Multiple-hosts Per Port

The multiple-hosts per port setting is appropriate when the ports are connected to more than one host node, such as when ports are connected to other Ethernet switches where there are multiple host nodes. With this setting selected, the switch continues sending multicast packets out a port even after it receives a leave request from a host node. This ensures that the remaining active host nodes on a port continue to receive the multicast packets. Only after all the host nodes connected to a switch port have transmitted leave requests, or have timed out, does the switch stop sending multicast packets out a port.

If the switch has a mixture of host nodes, that is, some connected directly to the switch and others through other Ethernet switches or hubs, you should select the multiple-hosts per port setting.

426

Enabling IGMP Snooping

The command to enable IGMP Snooping on the switch is the IP IGMP SNOOPING command in the Global Configuration mode. After you enter the command, the switch begins to build its multicast table as queries from the multicast router and reports from the host nodes arrive on its ports. To enable IGMP Snooping:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping
```

Configuring the IGMP Snooping Commands

This table lists the IGMP Snooping commands with the exception of the enable, disable, and display commands which are described in other sections of this chapter.

Table 40. IGMP Snooping Commands

To	Use This Command	Range
Clear all IGMP group membership records.	CLEAR IP IGMP	none
Specify the maximum number of multicast groups the switch will support.	IP IGMP LIMIT *multicastgroups*	0 to 255 multicast addresses
Specify the time period, in seconds, used by the switch to identify inactive host nodes and multicast routers.	IP IGMP QUERIER-TIMEOUT *timeout*	1 to 65535 seconds (default 255)
Disable the suppression of unknown multicast traffic.	IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST	none
Specify ports that are connected to multicast routers.	IP IGMP SNOOPING MROUTER INTERFACE *port*	none
Specify the IGMP host node topology.	IP IGMP STATUS SINGLE|MULTIPLE	none
Remove static multicast router ports and reactivate auto-detection of router ports.	NO IP IGMP SNOOPING MROUTER INTERFACE *port*	none

Most of the commands are found in the Global Configuration mode. The following examples illustrate the commands. The first example clears all IGMP group membership records on all VLANs:

```
awplus> enable
awplus(config)# clear ip igmp
```

For more information about this command, see "CLEAR IP IGMP" on page 434.

428

This example limits the switch to two multicast groups and specifies that there is only one host node per port:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp limit 2
awplus(config)# ip igmp status single
```

For more information about these commands, see "IP IGMP LIMIT" on page 435 and "IP IGMP STATUS" on page 441.

This example configures the switch to time out inactive host nodes after 50 seconds and designates port 4 as a multicast router port:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp querier-timeout 50
awplus(config)# ip igmp snooping mrouter interface port1.0.4
```

For more information about these commands, see "IP IGMP QUERIER-TIMEOUT" on page 436 and "IP IGMP SNOOPING MROUTER" on page 440.

This example disables the suppression of unknown multicast traffic:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping
awplus(config)# ip igmp snooping flood-unknown-mcast
```

For more information about this command, see "IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST" on page 438.

This example reactivates the auto-detection of multicast router ports by removing the static router port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping mrouter interface
port1.0.4
```

For more information about this command, see "NO IP IGMP SNOOPING MROUTER" on page 443.

Disabling IGMP Snooping

The command to disable IGMP Snooping on the switch is the NO IP IGMP SNOOPING command in the Global Configuration mode. To disable IGMP Snooping:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping
```

When IGMP Snooping is disabled, the switch floods the multicast packets on all ports, except on ports that receive the packets.

Displaying IGMP Snooping

To display the settings of IGMP Snooping and its status, use the SHOW IP IGMP SNOOPING command in the User Exec mode or Privileged Exec mode:

awplus# show ip igmp snooping

Here is an example of the information the command displays:

```
IGMP Snooping Configuration:
   IGMP Snooping Status ............... Enabled
   Host Topology ...................... Single-Host/Port
   Host/Router Timeout Interval ....... 255 seconds
   Maximum IGMP Multicast Groups ...... 64
   Router Port(s) ..................... Auto Detect

Router List:
VLAN ID     Port/Trunk ID  RouterIP          Exp. Time
----------------------------------------------------
1           port1.0.31     10.0.0.254        110

Host List:
Number of IGMP Multicast Groups: 2

MulticastGroup  VLAN ID Port/TrunkID HostIP        IGMP Ver Exp.Time
-------------------------------------------------------------------
0100.5e7f.ffff  1       port1.0.1    192.169.20.50 v3       200
0100.5e7f.ffff  1       port1.0.30   172.16.20.222 v2       45
0100.5e64.3201  1       port1.0.15   10.10.5.01    v1       161
```

Figure 87. SHOW IP IGMP SNOOPING

The information in the window is described in Table 42 on page 445.

432

Chapter 24
IGMP Snooping Commands

The IGMP snooping commands are summarized in Table 41 and are described in detail within the chapter.

Table 41. Internet Group Management Protocol Snooping Commands

Command	Mode	Description
"CLEAR IP IGMP" on page 434	Privileged Exec	Clears all IGMP group membership records.
"IP IGMP LIMIT" on page 435	Global Configuration	Specifies the maximum number of multicast addresses the switch is allowed to learn.
"IP IGMP QUERIER-TIMEOUT" on page 436	Global Configuration	Specifies the time period in seconds used by the switch to identify inactive host nodes and multicast routers.
"IP IGMP SNOOPING" on page 437	Global Configuration	Enables IGMP snooping on the switch.
"IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST" on page 438	Global Configuration	Disables the automatic suppression of unknown multicast traffic.
"IP IGMP SNOOPING MROUTER" on page 440	Global Configuration	Manually identifies the ports where multicast routers are connected.
"IP IGMP STATUS" on page 441	Global Configuration	Specifies the IGMP host node topology, of either single-host per port or multiple-host per port.
"NO IP IGMP SNOOPING" on page 442	Global Configuration	Disables IGMP snooping on the switch.
"NO IP IGMP SNOOPING MROUTER" on page 443	Global Configuration	Removes multicast router ports.
"SHOW IP IGMP SNOOPING" on page 444	Privileged Exec	Displays the parameter settings and operational details of IGMP snooping.

CLEAR IP IGMP

Syntax

```
clear ip igmp
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to clear all IGMP group membership records on all VLANs.

Example

This example clears all IGMP group membership records on all VLANs:

```
awplus> enable
awplus# clear ip igmp
```

IP IGMP LIMIT

Syntax

ip igmp limit *multicastgroups*

Parameter

multicastgroups
> Specifies the maximum number of multicast addresses the switch is allowed to learn. The range is 0 to 255 multicast addresses; the default is 64 addresses.

Mode

Global Configuration mode

Description

Use this command to specify the maximum number of multicast addresses the switch can learn. If your network has a large number of multicast groups, you can use this parameter to limit the number of multicast groups the switch supports.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Example

This example sets the maximum number of multicast groups on the switch to 25:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp limit 25
```

IP IGMP QUERIER-TIMEOUT

Syntax

```
ip igmp querier-timeout timeout
```

Parameters

timeout

Specifies the time period in seconds used by the switch to identify inactive host nodes and multicast routers. The range is from 0 to 65535 seconds. The default is 255 seconds. Setting the timeout to zero (0) disables the timer.

Mode

Global Configuration mode

Description

Use this command to specify the time period the switch uses to identify inactive host nodes and multicast routers. The time period is in seconds.

A host node is deemed inactive if the switch does not receive any IGMP reports from it for the duration of the timer. The switch stops transmitting multicast packets from a port of an inactive host node if there are no additional host nodes.

A multicast router is deemed inactive if the switch does not receive any queries from it for the duration of the timer.

The actual timeout may be 10 seconds less that the specified value. For example, a setting of 25 seconds can result in the switch classifying a host node or multicast router as inactive after only 15 seconds. A setting of 10 seconds or less can result in the immediate timeout of inactive host nodes or routers.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Example

This example sets the timeout for inactive host nodes and multicast routers to 400 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp querier-timeout 400
```

IP IGMP SNOOPING

Syntax

```
ip igmp snooping
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate IGMP snooping on the switch.

> ⚠️ **Caution**
> The IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST command is enabled by default when IGMP Snooping is activated. This may cause a slow-down of network data. If you want to disable flooding of unknown multicast packets, you must enter the NO IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST command.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Example

This example enables IGMP Snooping on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping
```

437

IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST

Syntax

```
ip igmp snooping flood-unknown-mcast
```

Parameter

None

Mode

Global Configuration mode

Description

This command disables the automatic suppression of unknown multicast traffic on the switch. By default, IGMP Snooping does not suppress all unknown multicast traffic except for IPv4 reserved addresses 224.0.0.1 through 224.0.0.255. When you enable the IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST command, all unknown multicast traffic is flooded before a join message. Once a join message occurs for a particular multicast destination, it is no longer "unknown" and, therefore, no longer floods.

Use the no version of this command, NO IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST, to enable the automatic suppression of unknown multicast traffic on the switch.

⚠ Caution
The IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST command is enabled by default when IGMP Snooping is activated. This may cause a slow-down of network data. If you want to disable flooding of unknown multicast packets, you must enter the NO IP IGMP SNOOPING FLOOD-UNKNOWN-MCAST command.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Examples

This example disables the automatic suppression of unknown multicast traffic on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping
awplus(config)# ip igmp snooping flood-unknown-mcast
```

This example enables the automatic suppression of unknown multicast traffic on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping flood-unknown-mcast
```

IP IGMP SNOOPING MROUTER

Syntax

```
ip igmp snooping mrouter interface port
```

Parameter

port

Specifies a port connected to a multicast router. You can specify more than one port.

Mode

Global Configuration mode

Description

Use this command to manually specify ports that are connected to multicast routers. Manually specifying multicast router ports deactivates auto-detect. To reactivate auto-detect, remove all static multicast router ports. For instructions, refer to "NO IP IGMP SNOOPING MROUTER" on page 443.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Example

This example identifies ports 14 and 15 as multicast router ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping mrouter interface
port1.0.14,port1.0.15
```

IP IGMP STATUS

Syntax

```
ip igmp status single | multiple
```

Parameters

single
> Activates the single-host per port setting, which is used when the ports on the switch have only one host node each.

multiple
> Activates the multiple-host per port setting, which is used when the ports have more than one host node.

Mode

Global Configuration mode

Description

Use this command to specify the IGMP host node topology. For background information, refer to "Host Node Topology" on page 426.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Examples

This example sets the host node topology to the single-host per port setting:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp status single
```

This example sets the host node topology to the multiple-host per port setting:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp status multiple
```

NO IP IGMP SNOOPING

Syntax

```
no ip igmp snooping
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to deactivate IGMP snooping on the switch.

When IGMP snooping is disabled, the switch floods multicast packets on all ports, except on ports that receive the packets.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping
```

NO IP IGMP SNOOPING MROUTER

Syntax

```
no ip igmp snooping mrouter interface port
```

Parameter

port
Specifies a multicast router port.

Mode

Global Configuration mode

Description

Use this command to remove static multicast router ports. Removing all multicast router ports activates auto-detect.

Confirmation Command

"SHOW IP IGMP SNOOPING" on page 444

Examples

This example removes port 3 as multicast router ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping mrouter interface
port1.0.3
```

SHOW IP IGMP SNOOPING

Syntax

show ip igmp snooping

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the IGMP snooping parameters. Figure 88 illustrates the information.

```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Enabled
  Host Topology ...................... Single-Host/Port
  Host/Router Timeout Interval ....... 255 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect

Router List:
VLAN ID      Port/Trunk ID  RouterIP          Exp. Time
----------------------------------------------------
1            port1.0.31     10.0.0.254        110

Host List:
Number of IGMP Multicast Groups: 2

MulticastGroup  VLAN ID Port/TrunkID HostIP         IGMP Ver Exp.Time
---------------------------------------------------------------------
0100.5e7f.ffff  1       port1.0.1    192.169.20.50  v3       200
0100.5e7f.ffff  1       port1.0.30   172.16.20.222  v2       45
0100.5e64.3201  1       port1.0.15   10.10.5.01     v1       161
```

Figure 88. SHOW IP IGMP SNOOPING Command

444

The information the command displays is explained in Table 42.

Table 42. SHOW IP IGMP SNOOPING Command

Parameter	Description
IGMP Snooping Configuration	
IGMP Snooping Status	The status of IGMP snooping on the switch. To enable or disable the feature, refer to "IP IGMP SNOOPING" on page 437 and "NO IP IGMP SNOOPING" on page 442, respectively.
Host Topology	The IGMP host node topology on the switch. The possible topologies are:
	singlehost— This is the single-host per port topology. This topology is appropriate when there is only one host node per port on the switch. This is the default setting.
	multihost— This is the multiple-host per port topology. This topology is appropriate when there is more than one host node per port on the switch.
	To set this parameter, refer to "IP IGMP STATUS" on page 441.
Host/Router Timeout Interval	The amount of time the switch uses to time out inactive host nodes and multicast routers. To set this parameter, refer to "IP IGMP QUERIER-TIMEOUT" on page 436.
Maximum IGMP Multicast Groups	The maximum number of multicast groups the switch supports. To set this parameter, refer to "IP IGMP LIMIT" on page 435.
Router Port(s)	The ports connected to multicast routers. The switch can learn the router ports automatically or you can assign them manually. To assign the ports manually, refer to "IP IGMP SNOOPING MROUTER" on page 440.
Router List	
VLAN ID	The ID numbers of the VLANs of the router ports.

445

Table 42. SHOW IP IGMP SNOOPING Command (Continued)

Parameter	Description
Port/Trunk ID	The port of a multicast router. If the switch learned a router on a port trunk, the trunk ID number, instead of a port number, is displayed.
Router IP	The IP addresses of the multicast routers.
Exp. Time	The number of seconds remaining before the switch times out a multicast router if there are no further IGMP queries from it.
Host List	
Number of IGMP Multicast Groups	The number of IGMP multicast groups that have active host nodes on the switch.
Multicast Group	The multicast addresses of the groups.
ID	The ID numbers of the VLANs of the host nodes.
Port/Trunk ID	The ports of the host nodes. If the host nodes are on port trunks, this field displays the trunk ID numbers instead of the port numbers.
HostIP	The IP addresses of the host nodes.
IGMP Ver.	The IGMP versions used by the host nodes.
Exp. Time	The number of seconds remaining before host nodes are timed out if they do not send IGMP reports.

Example

The following example displays the IGMP snooping parameters:

```
awplus# show ip igmp snooping
```

Chapter 25
Multicast Commands

The multicast commands are summarized in Table 43.

Table 43. Multicast Commands

Command	Mode	Description
"NO SWITCHPORT BLOCK EGRESS-MULTICAST" on page 448	Port Interface	Resumes forwarding egress multicast packets on ports.
"NO SWITCHPORT BLOCK INGRESS-MULTICAST" on page 449	Port Interface	Resumes forwarding ingress multicast packets on ports.
"SWITCHPORT BLOCK EGRESS-MULTICAST" on page 450	Port Interface	Blocks egress multicast packets on ports.
"SWITCHPORT BLOCK INGRESS-MULTICAST" on page 451	Port Interface	Blocks ingress multicast packets on ports.

NO SWITCHPORT BLOCK EGRESS-MULTICAST

Syntax

```
no switchport block egress-multicast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to resume forwarding of egress multicast packets on ports. By default, this is the default setting on all of the ports on the switch.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example resumes forwarding of egress multicast packets on port 19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.19
awplus(config-if)# no switchport block egress-multicast
```

NO SWITCHPORT BLOCK INGRESS-MULTICAST

Syntax

```
no switchport block ingress-multicast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to resume forwarding of ingress multicast packets on ports.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example resumes forwarding of ingress multicast packets on ports 2 and 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2,port1.0.8
awplus(config-if)# no switchport block ingress-multicast
```

SWITCHPORT BLOCK EGRESS-MULTICAST

Syntax

```
switchport block egress-multicast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to block egress multicast packets on ports. By default, all ports on the switch are set to *allow* multicast packets.

> **Note**
> This feature does not block multicast packets that have reserved multicast addresses in the range of 01:80:C2:00:00:00 to 01:80:C2:00:00:0F.

> **Note**
> If IGMP snooping is disabled on the switch, *all* reports are suppressed on a port even if you enable this command. By default, IGMP snooping is disabled on the switch. For more information about this feature, see Chapter 23, "Internet Group Management Protocol (IGMP) Snooping" on page 423.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example blocks egress multicast packets on ports 20 and 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20,port1.0.22
awplus(config-if)# switchport block egress-multicast
```

SWITCHPORT BLOCK INGRESS-MULTICAST

Syntax

```
switchport block ingress-multicast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to block ingress multicast packets on ports.

Note

This feature does not block multicast packets that have reserved multicast addresses in the range of 01:80:C2:00:00:00 to 01:80:C2:00:00:0F.

Note

If IGMP snooping is disabled on the switch, *all* reports are suppressed on a port even if you enable this command. By default, IGMP snooping is disabled on the switch. For more information about this feature, see Chapter 23, "Internet Group Management Protocol (IGMP) Snooping" on page 423.

Confirmation Command

"SHOW INTERFACE" on page 221.

Example

This example blocks ingress multicast packets on ports 12 to 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12-port1.0.18
awplus(config-if)# switchport block ingress-multicast
```

452

Section III
File System

This section contains the following chapters:

454

Chapter 26

File System

This chapter discusses the following topics:

Overview

The file system in the switch stores the following types of files:

❏ Boot configuration files

❏ Encryption key pairs

The file system has a flat directory structure. All the files are stored in the root directory. The file system does not support subdirectories.

Table 44. File Extensions and File Types

Extension	File Type
.cfg	Configuration file
.cer	Certificate file
.pem	Certificate enrollment request
.key	Public encryption key
.log	Event log

Copying Boot Configuration Files

Maintaining a history of the configuration settings of the switch can prove useful in the event you need to undo recent changes and return the device to an earlier configuration. The best way to compile a configuration history of the unit is by periodically copying the active boot configuration file.

The command for copying boot configuration files is the COPY command in the Privileged Exec mode. Here is the format:

```
copy sourcefile.cfg destinationfile.cfg
```

The SOURCEFILE parameter *s*pecifies the name of the boot configuration file you want to copy. The DESTINATIONFILE parameter specifies the name of the new copy. The name can be up to 16 alphanumeric characters and must include the extension ".cfg". Spaces are not allowed.

This command creates a copy of the configuration file "unit12.cfg" in the switch's file system and names the copy "unit24.cfg":

```
awplus# copy unit12.cfg unit24.cfg
```

> **Note**
> Allied Telesis recommends that you periodically upload the active boot configuration file of the switch to a network device, so that if the switch should fail and become inoperable, the uploaded files will be available to quickly configure its replacement. For instructions on how to upload boot configuration files, refer to Chapter 30, "File Transfer" on page 489.

Renaming Boot Configuration Files

To rename boot configuration files in the file system, use the MOVE command, found in the Privileged Exec mode. Here is the format:

move *filename1*.cfg *filename2*.cfg

The FILENAME1 variable is the name of the file to be renamed and the FILENAME2 variable is the file's new name. The filenames cannot contain spaces or special characters.

This example renames the "Sales2sw.cfg" boot configuration file to "unit12a.cfg:"

```
awplus> enable
awplus# move Sales2sw.cfg unit12a.cfg
```

Note
If you rename the active boot configuration file, you will have to designate another active boot configuration file before the switch will allow you to save new parameter settings. For instructions on how to designate the active boot configuration file, refer to "Specifying the Active Boot Configuration File" on page 473.

Note
If you rename the active boot configuration file and reset the switch, the switch restores the default settings to all its parameter settings.

458

Deleting Boot Configuration Files

If the file system becomes cluttered with unnecessary configuration files, you use the DELETE command in the Privileged Exec mode to delete them. The format of the command is:

```
delete filename.ext
```

This example deletes the configuration file "unit2a.cfg":

```
awplus# delete unit2a.cfg
```

> **Note**
> If you delete the active boot configuration file, you will have to designate another active boot configuration file before the switch will allow you to save new parameter settings. If you delete the active boot configuration file and reset the switch, the switch returns to its default settings. For instructions on how to designate the active boot configuration file, refer to "Specifying the Active Boot Configuration File" on page 473.

Displaying the Specifications of the File System

The User Exec mode and the Privileged Exec mode have a command that lets you display the size of the file system, the amount of free space, and the amount of space used by the files currently stored in the file system. It is the SHOW FILE SYSTEMS command. Here is an example of the information.

```
Size (b)   Free (b)   Type    Flags       Prefixes   S/D/V   Lcl/Ntwk  Avail
-----------------------------------------------------------------------------
2.0M       1.4M        flash   rw          /cfg/      static  local     Y
```

Figure 89. SHOW FILE SYSTEMS Command

The fields in the table are described in Table 46 on page 469.

Here is the command from the Privileged Exec mode:

```
awplus# show file systems
```

Listing the Files in the File System

To view the names of the files in the file system of the switch, use the DIR command in the Privileged Exec mode:

```
awplus# dir
```

The command does not accept wildcards.

Chapter 27
File System Commands

The file system commands are summarized in Table 45.

Table 45. File System Commands

Command	Mode	Description
"COPY" on page 464	Privileged Exec	Copies boot configuration files.
"DELETE" on page 465	Privileged Exec	Deletes boot configuration files from the file system.
"DELETE FORCE" on page 466	Privileged Exec	Deletes boot configuration files from the file system.
"DIR" on page 467	Privileged Exec	Lists the files in the file system.
"MOVE" on page 468	Privileged Exec	Renames files.
"SHOW FILE SYSTEMS" on page 469	Privileged Exec	Displays the amount of free and used memory in the file system.

COPY

Syntax

copy *sourcefile*.cfg *destinationfile*.cfg

Parameters

sourcefile.cfg
> Specifies the name of the boot configuration file you want to copy.

destinationfile.cfg
> Specifies the name of the new copy of the file. The filename can be from 1 to 16 alphanumeric characters. The extension must be ".cfg". Spaces and special characters are not allowed.

Mode

Privileged Exec mode

Description

Use this command to create copies of boot configuration files in the file system of the switch. Creating copies of the active boot configuration file is an easy way to maintain a history of the configurations of the switch. To display the name of the active boot configuration file, refer to "SHOW BOOT" on page 484.

If the destination filename is the same as the name of an existing file in the file system, the command overwrites the existing file.

Example

This command creates a copy of the boot configuration file "unit12.cfg" in the switch's file system and names the copy "unit12backup.cfg":

awplus# copy unit12.cfg unit12backup.cfg

DELETE

Syntax

delete *filename*.cfg

Parameter

filename.cfg
> Specifies the name of the boot configuration file to be deleted. You can use the wildcard "*" to replace any part of a filename to delete multiple configuration files.

Mode

Privileged Exec mode

Description

Use this command to delete boot configuration files from the file system in the switch. This command is equivalent to "DELETE FORCE" on page 466.

Note

If you delete the active configuration file, the switch recreates it the next time you issue the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command. To view the name of the active boot configuration file on the switch, refer to "SHOW BOOT" on page 484.

To view a list of the files in the file system, refer to "DIR" on page 467.

Examples

This command deletes the boot configuration file "unit12.cfg":

awplus# delete unit12.cfg

This command deletes all boot configuration files that start with "bldg":

awplus# delete bldg*.cfg

DELETE FORCE

Syntax

```
delete force filename.ext
```

Parameter

filename.ext
> Specifies the name of the boot configuration file to be deleted. You can use the wildcard "*" to replace any part of a filename to delete multiple configuration files.

Mode

Privileged Exec mode

Description

Use this command to delete boot configuration files from the file system in the switch. This command is equivalent to "DELETE" on page 465.

Note
If you delete the active configuration file, the switch recreates it the next time you issue the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command. To view the name of the active boot configuration file on the switch, refer to "SHOW BOOT" on page 484.

To view a list of the files in the file system, refer to "DIR" on page 467.

Examples

This command deletes the boot configuration file "production_sw.cfg":

```
awplus# delete force production_sw.cfg
```

This command deletes all boot configuration files that start with "unit":

```
awplus# delete force unit*.cfg
```

DIR

Syntax

```
dir
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to list the names of the files stored in the file system on the switch.

Example

The following command lists the file names stored in the file system:

```
awplus# dir
```

MOVE

Syntax

```
move filename1.cfg filename2.cfg
```

Parameters

filename1.cfg
> Specifies the name of the boot configuration file to be renamed.

filename2.cfg
> Specifies the new name for the file. The filename can be from 1 to 16 alphanumeric characters, not including the filename extension, which must be ".cfg". The filename cannot contain spaces or special characters.

Mode

Privileged Exec mode

Description

Use this command to rename boot configuration files in the switch's file system.

> **Note**
> If you rename the active boot configuration file, the switch recreates it the next time you issue the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command.

> **Note**
> If you rename the active boot configuration file and reset the switch without specifying a new active boot configuration file or issuing the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command, the switch returns to its default settings.

Example

This example renames the file "sw12.cfg" to "swrm102.cfg:"

```
awplus# move sw12.cfg swrm102.cfg
```

468

SHOW FILE SYSTEMS

Syntax

```
show file systems
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the specifications of the file system in the switch. An example is shown in Figure 90.

```
Size (b)  Free (b)   Type   Flags      Prefixes   S/D/V    Lcl/Ntwk  Avail
---------------------------------------------------------------------------
2.0M      1.4M       flash  rw         /cfg/      static   local     Y
```

Figure 90. SHOW FILE SYSTEMS Command

The fields are described in Table 46.

Table 46. SHOW FILE SYSTEMS Command

Parameter	Description
Size (B)	The total amount of flash memory in the switch. The amount is given in megabytes (M) or kilobytes (k).
Free (B)	The amount of unused flash memory in the switch. The amount is given in megabytes (M) or kilobytes (k).
Type	The type of memory. This is always "flash" for flash memory.
Flags	The file setting options. This is always "rw" for read-write.
Prefixes	The directory in which files are stored. This is always "cfg" for configuration file.

469

Table 46. SHOW FILE SYSTEMS Command (Continued)

Parameter	Description
S/D/V	The memory type: static, dynamic, or virtual.
Lcl/Ntwk	Whether the memory is located locally or via a network connection. This is always Local.
Y/N	Whether the memory is accessible: Y (yes), N (no), - (not appropriate)

Example

The following example displays the specifications of the file system:

```
awplus# show file systems
```

Chapter 28
Boot Configuration Files

This chapter discusses the following topics:

Overview

The changes that you make to the parameters settings of the switch are saved as a series of commands in a special file in the file system. The file is referred to as the active boot configuration file. This file is updated by the switch with your latest changes whenever you issue the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

Once the parameter settings are saved in the active boot configuration file, they are retained even when the switch is powered off or reset. This saves you from having to reconfigure the parameter settings every time you power off or reset the unit. The switch, as part of its initialization process whenever it is powered on or reset, automatically refers to this file to set its parameter settings.

You can store more than one boot configuration file in the file system on the switch, but only one file can be the active file at a time. The active boot configuration file is specified with the BOOT CONFIG-FILE command, in the Privileged Exec mode.

There are a couple of situations where you might want to specify a different active boot configuration file on the switch. You might want to reconfigure the switch with the settings in a new file that you downloaded into the file system. Or perhaps you want to restore a previous configuration on the switch, using a copy of an earlier version of the active boot configuration file.

Specifying the Active Boot Configuration File

To create or designate a new active boot configuration file for the switch, use the BOOT CONFIG-FILE command in the Global Configuration mode. Here is the format of the command;

```
boot config-file filename.cfg
```

The FILENAME.CFG parameter is the file name of the configuration file to act as the active boot configuration file for the switch. This can be the name of an entirely new file that does not exist yet in the file system, or an existing file. The filename can be from 1 to 16 alphanumeric characters and must include the ".cfg" extension. The filename is case sensitive. To verify the name of an existing file, use the DIR command in the Privileged Exec mode to display the names of the files in the file system.

The BOOT CONFIG-FILE command is unique from all the other commands that are used to configure the parameters on the switch. After you enter the command, the switch permanently remembers the filename of the new active boot configuration file, without you having to enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command. In fact, you probably will not want to enter either of those commands after you specify a new active boot configuration file, because that would cause the switch to overwrite the settings in the file with the current settings.

After you enter the command, it does one of two things, depending on whether the filename is of a new or an existing file. If the filename is of an entirely new boot configuration file, the switch automatically creates it, stores the current parameter settings in it, and finally designates it as the active boot configuration.

If you specify the filename of an existing boot configuration file in the file system, the switch marks it as the active boot configuration file, at which point you need to make a choice.

❏ To reconfigure the switch with the settings in the newly designated active boot configuration file, reset the switch with the REBOOT command in the Privileged Exec mode.

⚠️ **Caution**
The switch does not forward packets while it is initializing its management software. Some network traffic may be lost.

❏ To overwrite the settings in the file with the switch's current settings, enter the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

Here are a couple examples of the command. The first example creates a new active boot configuration file called "sw_product4.cfg":

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file sw_product4.cfg
```

After you enter the command, the switch creates the file in its file system, updates it with the current parameter settings, and finally marks it as the active boot configuration file. The file is now ready to store any new parameter settings you might make to the switch.

In this example, the settings of the switch are configured using a different boot configuration file in the file system. Perhaps it is an archive copy of an early configuration of the unit or perhaps a boot configuration file you downloaded from another switch. In either case, this will require rebooting the switch. The name of the file is "sw12_eng.cfg":

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file sw12_eng.cfg
awplus(config)# exit
awplus# reboot
```

474

Creating a New Boot Configuration File

It is a good idea to periodically make copies of the current configuration of the switch so that you can return the switch to an earlier configuration, if necessary. For this there is the COPY RUNNING-CONFIG command in the Privileged Exec mode. The command has this format:

```
copy running-config filename.cfg
```

The name of the new boot configuration file, specified with the FILENAME parameter, can be from 1 to 16 alphanumeric characters, not including the extension ".cfg". If you specify the name of an existing file, the new file overwrites the existing file.

It is important to understand that this command does not change the switch's active boot configuration file. That file remains unchanged. All this command does is create a new boot configuration file of the current parameter settings in the file system. If you want to change the active boot configuration file, use the BOOT CONFIG-FILE command, explained in "Specifying the Active Boot Configuration File" on page 473.

This example of the COPY RUNNING-CONFIG command creates a new boot configuration file called "sw_sales_archive.cfg" in the file system:

```
awplus> enable
awplus# copy running-config sw_sales_archive.cfg
```

Displaying the Active Boot Configuration File

To display the name of the active boot configuration file on the switch, go to the Privileged Exec mode and enter the SHOW BOOT command. Here is the command:

```
awplus# show boot
```

Here is an example of the information.

```
Current software   : v2.1.1
Current boot image : v2.1.1
Backup boot image  : Not set
Default boot config: /cfg/boot.cfg
Current boot config: /cfg/switch2.cfg (file exists)
```

Figure 91. SHOW BOOT Command

The "Current boot config" field displays the name of the active boot configuration file, which for the switch in the example is "switch2.cfg." The rest of the fields are defined in Table 48 on page 484.

476

Chapter 29

Boot Configuration File Commands

The boot configuration file commands are summarized in Table 47 and described in detail within the chapter.

Table 47. Boot Configuration File Commands

Command	Mode	Description
"BOOT CONFIG-FILE" on page 478	Global Configuration	Designates or creates a new active boot configuration file for the switch.
"COPY RUNNING-CONFIG" on page 480	Privileged Exec	Creates new boot configuration files that contain the current settings of the switch.
"COPY RUNNING-CONFIG STARTUP-CONFIG" on page 481	Privileged Exec	Saves the switch's current configuration to the active boot configuration file.
"ERASE STARTUP-CONFIG" on page 482	Privileged Exec	Returns the switch to its default settings.
"NO BOOT CONFIG-FILE" on page 483	Global Configuration	Designates the default BOOT.CFG file as the active boot configuration file on the switch.
"SHOW BOOT" on page 484	Privileged Exec	Displays the names of the active configuration file and the configuration file that was used by the switch during the last reset or power cycle.
"SHOW STARTUP-CONFIG" on page 486	Privileged Exec	Displays the contents of the active boot configuration file.
"WRITE" on page 487	Privileged Exec	Saves the switch's current configuration to the active boot configuration file.

BOOT CONFIG-FILE

Syntax

```
boot config-file filename.cfg
```

Parameter

filename
> Specifies the name of a boot configuration file that is to act as the active boot configuration file on the switch. The filename can be from 1 to 16 alphanumeric characters. The extension must be ".cfg".

Mode

Global Configuration mode

Description

Use this command to designate the active boot configuration file on the switch. The switch uses the file to save its parameter settings when you issue the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command, and to restore its parameter settings when you reset or power cycle the unit.

To create a new active boot configuration file, enter a new filename in the command. The command automatically creates the file, updates it with the current settings of the switch, and designates it as the active boot configuration file.

To specify an existing boot configuration file as the new active file on the switch, include the file's name in the command. The switch marks it as the active boot configuration file. Afterwards, do one of the following:

- ❑ To reconfigure the switch with the settings in the newly designated active boot configuration file, reset the switch with the REBOOT command in the Privileged Exec mode.

⚠️ **Caution**
The switch does not forward packets while it is initializing its management software. Some network traffic may be lost.

- ❑ To overwrite the settings in the file with the switch's current settings, enter the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

Confirmation Command

"SHOW BOOT" on page 484.

Examples

This example designates a file called "region2asw.cfg" as the switch's active configuration file. This example assumes that the file is completely new. The switch creates the file, with its current parameter settings, and then designates it as the active boot configuration file:

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file region2asw.cfg
```

This example designates the file "sw12a.cfg" as the switch's active configuration file. The example assumes that the file already exists in the file system of the switch and that you want to reconfigure the switch according to the settings in the file:

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file sw12a.cfg
awplus(config)# exit
awplus# reboot
```

This example designates the file "bldg4.cfg" as the active configuration file on the switch. This example assumes that instead of configuring the switch with the settings in the file, you want to overwrite the settings in the file with the current settings on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file bldg4.cfg
awplus(config)# exit
awplus# write
```

COPY RUNNING-CONFIG

Syntax

```
copy running-config filename.cfg
```

Parameter

filename

Specifies a name for a new boot configuration file. The name can be from 1 to 16 alphanumeric characters. The extension must be ".cfg".

Mode

Privileged Exec mode

Description

Use this command to create new boot configuration files. Stored in the file system on the switch, the files contain the current settings of the switch. You might use this command to create a backup copy of the switch's current configuration.

This command does not change the active boot configuration file. To designate a different file as the active boot configuration file on the switch, refer to "BOOT CONFIG-FILE" on page 478.

Confirmation Command

"DIR" on page 467

Example

This example creates a new boot configuration file called "salesunit2_archive.cfg".

```
awplus> enable
awplus# copy running-config salesunit2_archive.cfg
```

COPY RUNNING-CONFIG STARTUP-CONFIG

Syntax

```
copy running-config startup-config
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to update the active boot configuration file with the switch's current configuration, for permanent storage. When you enter the command, the switch copies its parameter settings into the active boot configuration file. The switch saves only those parameters that have been changed from their default settings.

Note
Parameter changes that are not saved in the active boot configuration file are discarded when the switch is powered off or reset.

To view the name of the active boot configuration file, see "SHOW BOOT" on page 484.

This command is equivalent to "WRITE" on page 487.

Example

The following example updates the active boot configuration with the switch's current configuration:

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

ERASE STARTUP-CONFIG

Syntax

```
erase startup-config
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to restore the default settings to all the parameters on the switch. Review the following information before using this command:

❒ This command does not delete the files in the switch's file system or the encryption keys in the key database. To delete those files, refer to "DELETE" on page 465 and "CRYPTO KEY DESTROY HOSTKEY" on page 1342.

❒ This command does not change the settings in the active boot configuration file. To return the active configuration file to the default settings, you must enter the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command after the switch reboots and after you have established a local management session. Otherwise, the switch reverts to the previous configuration the next time it is reset.

❒ To resume managing the switch, you must use the Console port. Remote management is not possible because the switch will not have a management IP address.

⚠️ **Caution**
This command causes the switch to reset. The switch will not forward network traffic while it initializes its management software. Some network traffic may be lost.

Example

This example restores all the parameters on the switch to their default values:

```
awplus> enable
awplus# erase startup-config
```

482

NO BOOT CONFIG-FILE

Syntax

```
no boot config-file
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to configure the switch with the settings in the default BOOT.CFG file.

> ⚠️ **Caution**
> This command causes the switch to reset. It does not forward network traffic while it initializes the management software. Some network packets may be lost.

After the switch finishes initializing its management software, it uses the BOOT.CFG file to configure its parameter settings. To overwrite the settings in the active boot configuration file with the switch's current settings, enter the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

This command does not return the switch to its default settings if, at some earlier time, you used the BOOT.CFG file as the activate boot configuration file on the switch. To restore the default settings to the switch, refer to "ERASE STARTUP-CONFIG" on page 482.

Example

This example configures the switch with the settings in the default BOOT.CFG file:

```
awplus> enable
awplus# configure terminal
awplus(config)# no boot config-file
```

SHOW BOOT

Syntax

show boot

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the name of the active boot configuration file and the version numbers of the management software and bootloader. Figure 92 is an example of the information.

```
Current software: v2.1.1
Current boot image: v2.1.1
Default boot config: /cfg/boot.cfg
Current boot config: /cfg/switch2.cfg (file exists)
```

Figure 92. SHOW BOOT Command

The fields are described in Table 48.

Table 48. SHOW BOOT Command

Field	Description
Current software	The version number of the AlliedWare Plus Management Software on the switch.
Current boot image	The version number of the bootloader.
Default boot config	The name of the boot configuration file used by the switch to configure its parameters after "NO BOOT CONFIG-FILE" on page 483. This parameter cannot be changed.
Current boot config	The name of the active boot configuration file on the switch.

Example

This command displays the name of the active boot configuration file and the version numbers of the management software and bootloader.

```
awplus# show boot
```

SHOW STARTUP-CONFIG

Syntax

```
show startup-config
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the contents of the active boot configuration file.

Example

The following example displays the contents of the active boot configuration file:

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

WRITE

Syntax

write

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to update the active boot configuration file with the switch's current configuration, for permanent storage. When you enter the command, the switch copies its parameter settings into the active boot configuration file. The switch saves only those parameters that have been changed from their default settings.

Note

Parameter changes that are not saved in the active boot configuration file are discarded when the switch is powered off or reset.

To view the name of the active boot configuration file, see "SHOW BOOT" on page 484.

This command is equivalent to "COPY RUNNING-CONFIG STARTUP-CONFIG" on page 481.

Example

The following example updates the active boot configuration file with the switch's current configuration:

awplus# write

Chapter 30

File Transfer

This chapter discusses the following topics:

❐ "Overview" on page 490

❐ "Uploading or Downloading Files with TFTP" on page 491

❐ "Uploading or Downloading Files with Zmodem" on page 495

❐ "Downloading Files with Enhanced Stacking" on page 498

Overview

This chapter discusses how to download files onto the switch and upload files onto the switch. You can download the following file types to the switch:

❒ New versions of the management software

❒ Boot configuration files (Refer to Chapter 28, "Boot Configuration Files" on page 471.)

❒ Public or private CA certificates (Refer to Chapter 86, "Secure HTTPS Web Browser Server" on page 1363.)

You can upload following file types from the switch:

❒ Boot configuration files

❒ CA certificate requests

❒ Technical support text files (Refer to "SHOW TECH-SUPPORT" on page 1444.)

You can use Zmodem or TFTP to transfer files. You must use local management sessions of the switch to transfer files using Zmodem. For TFTP, you can use local management sessions, or remote Telnet or SSH sessions. You can also transfer files with enhanced stacking.

Uploading or Downloading Files with TFTP

❐ "Downloading New Management Software with TFTP" next

❐ "Downloading Files to the Switch with TFTP" on page 492

❐ "Uploading Files from the Switch with TFTP" on page 493

These procedures can be performed from a local management session or a remote Telnet or SSH session.

Here are the TFTP requirements:

❐ The switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ The switch's management IP address must include a default gateway if the switch and the TFTP server are members of different networks. The default gateway must specify the IP address of the first hop to the network of the TFTP server.

❐ There must be a TFTP server on your network.

❐ The TFTP server must be active.

Downloading New Management Software with TFTP

To use TFTP to download new management software to the switch:

⚠️ **Caution**
This procedure causes the switch to reset. The switch does not forward network traffic while it writes the new software to flash memory and initializes the software. Some network traffic may be lost.

1. Obtain the new management software from the Allied Telesis web site and store it on the TFTP server on your network. For information on how to obtain management software from Allied Telesis, refer to "Contacting Allied Telesis" on page 40.

2. Start a local or remote management session on the switch.

3. To view the current version number of the management software on the unit to determine whether the switch needs the new firmware, use the SHOW SYSTEM command in the User Exec mode or the SHOW SWITCH command in the Privileged Exec mode.

4. The command for downloading files to the switch with TFTP is the COPY TFTP FLASH command in the Privileged Exec mode. Here is the format of the command:

```
copy tftp flash ipaddress filename.img
```

The IPADDRESS parameter is the IP address of the TFTP server, and the FILENAME parameter is the name of the new management software file to be downloaded to the switch from the TFTP server. The filename must include the ".img" extension and cannot contain spaces.

In this example of the command, the IP address of the TFTP server is 149.11.124.5 and the filename of the new management software to be downloaded from the server is "at-9000_sw.img":

```
awplus# copy tftp flash 149.11.124.5 AT-9000_sw.img
```

After receiving the entire file from the TFTP server, the switch compares the version numbers of the new image file and its current management software. If the new image file has an earlier or the same version number as the current management software, the switch cancels the update procedure. If the new image file has a newer version number, the switch writes the file into flash memory and then resets.

5. Wait for the switch to write the new management software to flash memory.

6. To resume managing the switch, start a new management session after the switch has reset.

7. To confirm the new management software on the switch, use the SHOW SYSTEM command in the User Exec mode or the SHOW SWITCH command in the Privileged Exec mode to check the version number of the management software on the switch.

Downloading Files to the Switch with TFTP

To use TFTP to download boot configuration files or CA certificates to the switch:

1. Store the file on the TFTP server on your network.

2. Start a local management session or a remote Telnet or SSH management session on the switch.

3. The command for downloading files to the switch with TFTP is the COPY TFTP FLASH command in the Privileged Exec mode. Here is the format of the command:

```
copy tftp flash ipaddress filename.exe
```

The IPADDRESS parameter is the IP address of the TFTP server. The FILENAME parameter is the name of the file you want to download from the TFTP server to the switch. The filename extension must be ".cfg" for boot configuration files and ".pem" for CA certificates. The filename cannot contain spaces.

In this example of the command, the IP address of the TFTP server is 152.34.67.8, and the filename of the boot configuration to be downloaded from the server is "switch2a.cfg":

```
awplus# copy tftp flash 152.34.67.8 switch2a.cfg
```

After receiving the entire file, the switch stores it in the file system.

4. To confirm that the switch received the file, use the DIR command in the Privileged Exec mode to list the files in the file system.

5. If you downloaded a boot configuration file that you want to designate as the active boot configuration file on the switch, use the BOOT CONFIG-FILE command in the Global Configuration mode:

```
boot config-file filename.cfg
```

This example of the command designates "switch1a.cfg" as the switch's new active boot configuration file:

```
awplus# configure terminal
awplus(config)# boot config-file switch1a.cfg
```

6. At this point, do one of the following:

    ❐ To configure the switch using the settings in the newly designated active boot configuration file, reset the switch with the REBOOT command in the Privileged Exec mode.

    ⚠ **Caution**

    The switch does not forward packets while initializing the management software. Some network traffic may be lost.

    ❐ To overwrite the settings in the file with the switch's current settings, enter the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

Uploading Files from the Switch with TFTP

You can upload three types of files from the file system of the switch:

❐ Boot configuration files (Refer to Chapter 28, "Boot Configuration Files" on page 471.)

❐ CA certificate requests (Refer to Chapter 86, "Secure HTTPS Web Browser Server" on page 1363.)

❐ Technical support text files (Refer to "SHOW TECH-SUPPORT" on page 1444.)

To upload a file from the file system of the switch using TFTP:

1. Start a local or remote management session on the switch.

2. Use the DIR command in the Privileged Exec mode to confirm the name of the file you want to upload from the file system in the switch.

3. The command for uploading files from the switch with TFTP is the COPY FLASH TFTP command in the Privileged Exec mode. Here is the format of the command:

```
copy flash tftp ipaddress filename
```

The IPADDRESS parameter is the IP address of the TFTP server residing on your network. The FILENAME parameter is the name of the file to be uploaded from the switch to the TFTP server. The filename can not contain spaces and must include the appropriate extension.

This example of the command uploads the boot configuration file "sw_unit_12.cfg" from the file system to a TFTP server that has the IP address 123.32.45.3:

```
awplus# copy flash tftp 123.32.45.3 sw_unit_12.cfg
```

This example uploads the technical support file "tech-support-20100601091645.txt" from the file system to a TFTP server that has the IP address 149.152.201.25:

```
awplus# copy flash tftp 149.152.201.25 tech-support-
20100601091645.txt
```

The upload should take only a few moments. The switch displays the Privileged Exec prompt again when it is finished uploading the file.

Uploading or Downloading Files with Zmodem

❏ "Downloading Files to the Switch with Zmodem" next

❏ "Uploading Files from the Switch with Zmodem" on page 496

> **Note**
> You may not use Zmodem to download new versions of the management software to the switch. For that, you must use TFTP.

Downloading Files to the Switch with Zmodem

You may use Zmodem to download boot configuration files and encryption key certificates to the file system in the switch. To download a file using Zmodem:

1. Store the boot configuration file on the terminal or workstation you intend to use during the local management session of the switch.

2. Start a local management session on the switch. For instructions, refer to "Starting a Local Management Session" on page 66.

3. Enter this command in the Privileged Exec mode:

    ```
    awplus# copy zmodem
    ```

    You will see this prompt:

    ```
    Waiting to receive ...
    ```

4. Use your terminal or terminal emulator program to begin the download. The download must be Zmodem.

    After receiving the entire file, the switch stores it in the file system.

5. To confirm that the switch received the file, use the DIR command in the Privileged Exec mode to list the files in the file system.

6. If you downloaded a boot configuration file and want to designate it as the active boot configuration file on the switch, use the BOOT CONFIG-FILE command in the Global Configuration mode:

    ```
    boot config-file filename.cfg
    ```

    This example of the command designates "switch2a.cfg" as the switch's new active boot configuration file:

    ```
    awplus# configure terminal
    awplus(config)# boot config-file switch2a.cfg
    ```

7. At this point, do one of the following:

❑ To configure the switch using the settings in the newly designated active boot configuration file, reset the switch with the REBOOT command in the Privileged Exec mode.

⚠ **Caution**

The switch does not forward packets while it is initializing its management software. Some network traffic may be lost.

❑ To overwrite the settings in the file with the switch's current settings, enter the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command in the Privileged Exec mode.

Uploading Files from the Switch with Zmodem

Here are the three types of files you can upload from the file system of the switch:

❑ Boot configuration files (Refer to Chapter 28, "Boot Configuration Files" on page 471.)

❑ CA certificate requests (Refer to Chapter 86, "Secure HTTPS Web Browser Server" on page 1363.)

❑ Technical support text files (Refer to "SHOW TECH-SUPPORT" on page 1444.)

To upload a file from the switch using Zmodem:

1. Start a local management session on the switch. For instructions, refer to "Starting a Local Management Session" on page 66.

2. Use the DIR command in the Privileged Exec mode to confirm the name of the file you want to upload from the file system of the switch.

3. Enter the COPY command in the Privileged Exec mode to upload the file. Here is the format of the command:

copy *filename* zmodem

The FILENAME parameter is the name of the configuration file you want to upload from the switch. The filename can not contain spaces and must include the appropriate extension.

This example of the command uploads the configuration file "bldg2_sw.cfg":

awplus# copy bldg2_sw.cfg zmodem

This example of the command uploads the technical support text file "tech-support-20100718120918.txt:"

awplus# copy tech-support-20100718120918.txt zmodem

After you enter the command, the switch displays this message:

```
Waiting to send ...
```

4. Use your terminal or terminal emulator program to begin the upload. The upload must be Zmodem. The upload should take only a few moments. The upload is finished when the Privileged Exec prompt is displayed again.

Downloading Files with Enhanced Stacking

If you are using the enhanced stacking feature, you can automate the process of updating the management software in the switches by having the command switch download its management software to the other switches in the stack.

⚠️ **Caution**

The switch automatically resets when it receives a new version of the management software. It does not forward network traffic while it writes the new software to flash memory and initializes the software. Some network traffic may be lost.

To update the management software of the switches in an enhanced stack:

1. Update the management software on the command switch of the enhanced stack by performing one of the previous procedures in this chapter.

2. After you have updated the management software on the command switch, start a new local or remote session on it.

   Issue the SHOW ESTACK REMOTELIST command in the Privileged Exec mode to display all the switches in the enhanced stack, except for the command switch. Here is an example of the display.

```
Searching for slave devices. Please wait...

Num    MAC Address          Name          Mode      Version    Model
----------------------------------------------------------------------
01     00:21:46:A7:B4:04    Production..  Slave     v1.0.0     AT-9000/28
02     00:21:46:A7:B4:43    Marketing     Slave     v1.0.0     AT-9000/28SP
03     00:30:84:00:00:02    Tech Suppo..  Slave     v1.0.0     AT-9000/52
```

Figure 93. SHOW ESTACK REMOTELIST

3. To have the command switch upload its management software to one or more of the other switches in the stack, enter the UPLOAD IMAGE REMOTELIST command in the Global Configuration mode. The command does not have any parameters. After you enter the command, this prompt is displayed:

```
Remote switches will reboot after load is complete.
Enter the list of switches ->
```

498

4. Enter the ID numbers of the switches to receive the management software from the command switch. The ID numbers are the numbers in the Num column in the SHOW ESTACK REMOTELIST command. You can update more than one switch at a time. For example, to update switches 1 and 2 in Figure 93 on page 498, you would enter:

```
Remote switches will reboot after load is complete.
Enter the list of switches -> 1,2
```

The command switch starts the download process with the first switch. After downloading its management software to that switch, it repeats the process with the next switch, and so on.

After a switch has received from the command switch the entire management software file, it compares the version numbers of the new image file and its current management software. If the new image file has an earlier or the same version number as the current management software, it cancels the update procedure. If the new image file has a newer version number, the switch writes the file into flash memory and then resets.

Chapter 31
File Transfer Commands

The file transfer commands are summarized in Table 49 and described in detail within the chapter.

Table 49. File Transfer Commands

Command	Mode	Description
"COPY FILENAME ZMODEM" on page 502	Privileged Exec	Uses Zmodem to upload files from the file system in the switch.
"COPY FLASH TFTP" on page 503	Privileged Exec	Uses TFTP to upload files from the switch.
"COPY TFTP FLASH" on page 504	Privileged Exec	Uses TFTP to download new versions of the management software, boot configuration files, or CA certificates to the switch.
"COPY ZMODEM" on page 506	Privileged Exec	Uses Zmodem to download new boot configuration files or CA certificates to the switch.
"UPLOAD IMAGE REMOTELIST" on page 507	Global Configuration	Uses enhanced stacking to download the management software on the command switch to other switches.

COPY FILENAME ZMODEM

Syntax:

copy *filename*.cfg zmodem

Parameters

filename
> Specifies the filename of a configuration file to upload from the file system in the switch. The filename cannot contain spaces and include the extension ".cfg". You can specify one filename.

Mode

Privileged Exec mode

Description

Use this command together with a Zmodem utility to upload boot configuration files from the file system in the switch to your terminal or computer. This command must be performed from a local management session. For instructions on how to use this command, refer to "Uploading Files from the Switch with Zmodem" on page 496.

Example

This example uploads the configuration file "eng_sw.cfg" from the file system in the switch:

awplus> enable
awplus# copy eng_sw.cfg zmodem

This message is displayed:

Waiting to send ...

Use your Zmodem utility to transfer the file to your terminal or computer. The upload method must be Zmodem.

COPY FLASH TFTP

Syntax

```
copy flash tftp ipaddress filename
```

Parameters

ipaddress

Specifies the IP address of a TFTP server on your network.

filename

Specifies the filename of a configuration file to upload from the file system in the switch to a TFTP server. The filename cannot contain spaces and must include the extension ".cfg". You can specify one filename.

Mode

Privileged Exec mode

Description

Use this command to upload configuration files from the file system in the switch to a TFTP server on your network. You can perform the command from a local management session or a remote Telnet or SSH management session. For instructions on how to use this command, refer to "Uploading Files from the Switch with TFTP" on page 493.

Example

This example uploads the configuration file "west_unit.cfg" from the file system in the switch to a TFTP server that has the IP address 149.22.121.45:

```
awplus> enable
awplus# copy flash tftp 149.22.121.45 west_unit.cfg
```

503

COPY TFTP FLASH

Syntax

```
copy tftp flash ipaddress filename
```

Parameters

ipaddress
> Specifies the IP address of a TFTP server on your network.

filename
> Specifies the filename of the file on the TFTP server to download to the switch. The file can be a new version of the management software, a boot configuration file or a CA certificate. The filename extensions are ".img" for management software, ".cfg" for boot configuration files, and ".pem" for CA certificates. The filename cannot contain spaces. You can specify one filename.

Mode

Privileged Exec mode

Description

Use this command to download new versions of the management software, boot configuration files, or CA certificates to the switch, from a TFTP server on your network. You may perform the command from a local management session or a remote Telnet or SSH management session. For instructions on how to use this command, refer to the following procedures:

❐ "Downloading New Management Software with TFTP" on page 491
❐ "Downloading Files to the Switch with TFTP" on page 492

> ⚠ **Caution**
> Downloading new management software causes the switch to reset. The switch does not forward network traffic while it writes the new software to flash memory and initializes the software. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost.

Examples

This example downloads the new management software file "at9000_app.img" to the switch from a TFTP server that has the IP address 149.22.121.45:

```
awplus> enable
awplus# copy tftp flash 149.22.121.45 at9000_app.img
```

This example downloads the boot configuration file "sw12a.cfg" to the switch from a TFTP server with the IP address 112.141.72.11:

```
awplus> enable
awplus# copy tftp flash 112.141.72.11 sw12a.cfg
```

COPY ZMODEM

Syntax

```
copy zmodem
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command together with a Zmodem utility to download boot configuration files or CA certificates to the file system in the switch. This command must be performed from a local management session. For instructions on how to use this command, refer to "Downloading Files to the Switch with Zmodem" on page 495.

> **Note**
> You may not use Zmodem to download new versions of the management software to the switch. For that, you must use TFTP.

Examples

```
awplus> enable
awplus# copy zmodem
```

The source file is not specified when downloading files with Zmodem. After you enter the command, the management software displays this message:

```
Waiting to receive.
```

Start the transfer by selecting the file with the Zmodem utility on your terminal or computer.

UPLOAD IMAGE REMOTELIST

Syntax

upload image remotelist

Parameters

None

Mode

Global Configuration mode

Description

Use this command to download the management software on the command switch to other switches in an enhanced stack. For background information on enhanced stacking, refer to Chapter 19, "Enhanced Stacking" on page 365. For instructions on how to use this command, refer to "Uploading the Management Software from the Command Switch to Member Switches" on page 385.

⚠️ **Caution**
Downloading new management software causes the switch to reset. The switch does not forward network traffic while it writes the new software to flash memory and initializes the software. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost.

Example

The following example downloads the management software of the command switch to other switches:

upload image remotelist

Section IV
Event Messages

This section contains the following chapters:

510

Chapter 32
Event Log

This chapter covers the following topics:

❑ "Overview" on page 512

❑ "Displaying the Event Log" on page 513

❑ "Clearing the Event Log" on page 514

Overview

A managed switch is a complex piece of computer equipment that includes both hardware and software components. Multiple software features operate simultaneously, inter-operating with each other and processing large amounts of network traffic. It is often difficult to determine exactly what is happening when a switch appears not to be operating normally, or what happened when a problem occurred.

The operation of the switch can be monitored by viewing the event messages generated by the device. These events and the vital information about system activity that they provide can help you identify and solve system problems.

The events are stored by the switch in an event log, in temporary memory. The events in the log are discarded whenever you reset or power cycle the switch.

The event messages include the following information:

- ◻ The time and date of the event
- ◻ The severity of the event
- ◻ The management module that generated the event
- ◻ An event description

512

Displaying the Event Log

There are two commands to display the messages stored in the event log. Both display the same messages and both are found in the Privileged Exec mode. The only difference is that one displays the messages from oldest to newest and the other from newest to oldest. The first command is the SHOW LOG command. If you are more interested in the older messages, this is the command to use. Here it is:

awplus# show log

The messages are displayed one screen at a time. To cancel the log, type 'q' for quit. Here is an example of the log.

```
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
----------------------------------------------------------------------
2010 Jan 15 14:39:04 user.information awplus stp: Set Configuration succeeded
2010 Jan 15 14:39:04 user.information awplus stp: Set Configuration succeeded
2010 Jan 15 14:39:04 user.information awplus stp: Disabled Spanning Tree
2010 Jan 15 14:39:04 user.information awplus stp: Active protocol changed to STP
```

Figure 94. SHOW LOG Command

The columns are described in Table 52 on page 521.

If you happen to be interested in the newer messages, use the SHOW LOG REVERSE command, instead. You will see the same messages, but the newest are displayed first.

513

Clearing the Event Log

To clear all the messages from the event log, use the CLEAR LOG BUFFERED command in the Privileged Exec mode. Here is the command:

```
awplus# clear log buffered
```

Chapter 33

Event Log Commands

The event log commands are summarized in Table 50 and described in detail within this chapter.

Table 50. Event Log Commands

Command	Mode	Description
"CLEAR LOG BUFFERED" on page 516	Privileged Exec	Deletes all entries in the event log.
"LOG BUFFERED" on page 517	Global Configuration	Specifies the types of event messages to be stored in the event log.
"NO LOG BUFFERED" on page 519	Global Configuration	Cancels the settings set by the LOG BUFFERED command.
"SHOW LOG" on page 521	Privileged Exec	Displays the event messages in the buffered log from oldest to newest.
"SHOW LOG CONFIG" on page 524	Privileged Exec	Displays the configuration of the event logs.
"SHOW LOG REVERSE" on page 526	Privileged Exec	Displays the event messages in the buffered log from newest to oldest.
"SHOW LOG TAIL" on page 527	Privileged Exec	Displays a limited number of the event messages in the buffered log.

515

CLEAR LOG BUFFERED

Syntax

```
clear log buffered
```

Parameters

None.

Mode

Privileged Exec mode

Description

Use this command to delete the event messages in the event log.

Confirmation Command

"NO LOG BUFFERED" on page 519

Example

The following command deletes the event messages in the event log:

```
awplus> enable
awplus# clear log buffered
```

516

LOG BUFFERED

Syntax

```
log buffered level level program program
```

Parameters

level	Specifies the minimum severity level of the event messages to be stored in the event log. The log stores the messages of the specified level and all higher levels. For instance, if you specify level 4, the log stores the messages for levels 0 and 4. The available severity levels are listed in Table 51. The default level 6 causes the log to store messages with the severity level 0, 4, or 6.
program	Specifies the event messages of a particular management software module. The modules are listed in Table 53 on page 522. To specify more than one module, separate the modules with commas.

Mode

Global Configuration mode

Description

Use this command to specify the types of event messages to be stored in the event log. You can specify the messages by severity level, management software module, or both. The available severity levels are listed in Table 51.

Table 51. Event Message Severity Levels

Severity	Description
0	Emergency message
4	Warning message
6	Informational message
7	Debug message

The management software modules are listed in Table 53 on page 522.

Confirmation Command

"SHOW LOG CONFIG" on page 524

Examples

This example configures the log to save event messages that have the severity level 0 or 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# log buffered level 4
```

This example configures the event log to save event messages that are generated by IGMP snooping (IGMPSNOOP), LACP (LACP) and port configuration (PCFG):

```
awplus> enable
awplus# configure terminal
awplus(config)# log buffered program igmpsnoop,lacp,
pcfg
```

This example configures the event log to save event messages that have the severity level 0 or 4 and that are generated by 802.1 port-based network access control (PACCESS) or GARP (GARP):

```
awplus> enable
awplus# configure terminal
awplus(config)# log buffered level 4 program paccess,garp
```

This example restores the event log to its default settings so that it saves messages with a severity level of 0, 4, or 6, from all management software modules:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log buffered
```

518

NO LOG BUFFERED

Syntax

```
no log buffered [level level]|[program program]|
[msgtext msgtext]
```

Parameters

level

Specifies the severity level setting.

program

Specifies the management software module setting. To specify more than one module, separate the modules with commas.

msgtext

Specifies a text string setting.

Mode

Global Configuration mode

Description

Use this command to cancel the settings set by the log buffered command. You can cancel a setting individually by specifying a parameter. If you do not specify any parameters, the command cancels all the settings and restores the default settings for the buffered log.

Confirmation Command

"SHOW LOG CONFIG" on page 524

Example

This example cancels the settings and restores the default settings for the buffered log:

```
awplus# no log buffered
```

This example cancels only the setting of MAC and keeps other settings so that the switch sends all messages that have a minimum severity level of 4 and that are generated by the IP program:

```
awplus# show log config
```

519

```
OUtputID  Type       Status    Details
-------------------------------------------------------------------------------------------------------
1         Temporary  Enabled   Wrap on Full. Filter: Level 4 program MAC, IP
```

```
awplus# configure terminal
awplus(config)# no log buffered Program mac
```

SHOW LOG

Syntax

show log

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the messages in the buffered event log. The event messages are displayed from oldest to newest, one screen at a time. To cancel the display, type 'q' for quit. You cannot filter the log for specific types of messages. An example of the log is shown in Figure 95.

```
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2010 Jan 15 14:39:04 user.information awplus stp: Set Configuration succeeded
2010 Jan 15 14:39:04 user.information awplus stp: Set Configuration succeeded
2010 Jan 15 14:39:04 user.information awplus stp: Disabled Spanning Tree
2010 Jan 15 14:39:04 user.information awplus stp: Active protocol changed to STP
```

Figure 95. SHOW LOG Command

The columns in the log are described here:

Table 52. SHOW LOG Command

Parameter	Description
Date/Time	The date and time the message was entered in the event log.
Facility	This is always "user."
Severity	The severity of the message. The severity levels are: ❒ Information: Useful information that can be ignored during normal operation. ❒ Error: Switch operation is severely impaired.

Table 52. SHOW LOG Command

Parameter	Description
Severity (continued)	❒ Warning: The issue reported by the message may require manager attention. ❒ Debug: Messages intended for technical support and software development.
Program	The module listed in Table 53 that generated the event message.
Message	The event message.

Table 53 lists the modules and their abbreviations.

Table 53. Management Software Modules

Module Name	Description
ALL	All management software modules
ACL	Port access control list
CFG	Switch configuration
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	System IP configuration
LACP	Link Aggregation Control Protocol
MAC	MAC address table
PACCESS	802.1x port-based access control
PCFG	Port configuration

Table 53. Management Software Modules

Module Name	Description
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	MAC address-based port security
PTRUNK	Static port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RTC	Real-time clock
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree and Rapid Spanning protocols
SYSTEM	Hardware status; manager and operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	Telnet
TFTP	TFTP
TIME	System time and SNTP
VLAN	Port-based, tagged and MAC address-based VLANs
WAT	Watchdog timer

Example

The following command displays the messages in the event log:

```
awplus# show log
```

SHOW LOG CONFIG

Syntax

show log config

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the configuration of the event log.

awplus# show log config

```
Permanent log:
 Status ................ Enable
   Filter:
   Level .............. Informational
   Program ............ All
   Message Text .......
Buffered log:
 Status ................ Enable
   Filter:
   Level .............. Informational
   Program ............ All
   Message Text .......
```
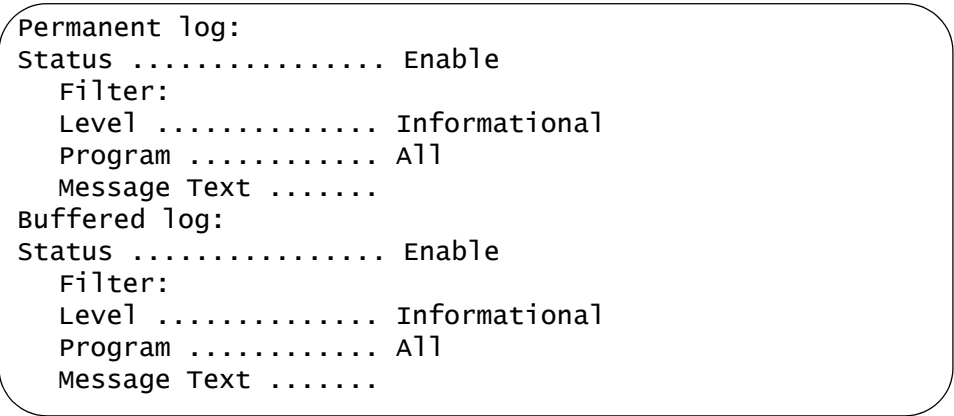
Figure 96. SHOW LOG CONFIG Command

The fields in the display are described here:

Table 54. SHOW LOG CONFIG Command

Field	Description
Level	The severity levels of the messages to be stored in the log. The default is level 6, Informational, and higher. The levels are defined in Table 51 on page 517.

Table 54. SHOW LOG CONFIG Command

Field	Description
Program	The software module messages to be stored in the log. The modules are listed in Table 53 on page 522. The default is all modules.
Message Text	Text that identifies the messages to be stored in the log.

This command is also used to view the configuration of the syslog client. For information, refer to "SHOW LOG CONFIG" on page 541 in Chapter 35, "Syslog Client Commands" on page 537.

Example

The following command displays the configuration of the event log:

```
awplus# show log config
```

SHOW LOG REVERSE

Syntax

```
show log reverse
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the event messages in the buffered log from newest to oldest. This command and the SHOW LOG command display the same messages, but in different order. The SHOW LOG command displays the messages from oldest to newest. To cancel the display, type 'q' for quit. You cannot filter the log for specific types of messages. For an example and description of the log, refer to Figure 95 on page 521 and Table 52 on page 521.

Example

This command displays the event messages in the buffered log from newest to oldest messages:

```
awplus# show log reverse
```

SHOW LOG TAIL

Syntax

show log tail [*number*]

Parameter

number
> Specifies the number of event messages to display. The range is 10 to 250 messages. The default is 10 messages.

Mode

Privileged Exec mode

Description

Use this command to display the most recent event messages in the buffered event log. The NUMBER parameter is used to specify the number of messages to display. The messages are displayed from oldest to newest. For an example and description of the log, refer to Figure 95 on page 521 and Table 52 on page 521.

Examples

This example displays the 10 most resent event messages in the buffered log. The messages are displayed from oldest to newest:

awplus# show log tail

This example displays the 30 most recent event messages:

awplus# show log tail 30

Chapter 34

Syslog Client

This chapter covers the following topics:

529

Overview

The switch has a syslog client. The client enables the switch to send its event messages to syslog servers on your network, for permanent storage.

To store the switch's event messages on a syslog server, you have to create a syslog server definition. The contents of a definition consist of an IP address of a syslog server and other information, such as the types of event messages the switch is to send.

Here are the guidelines to the syslog client:

❒ You can define up to 19 syslog server definitions.

❒ The switch must have a management IP address. For instructions, refer to "Adding a Management IP Address" on page 72 or Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The syslog servers must be members of the same subnet as the management IP address of the switch, or must be able to access the subnet through routers or other Layer 3 devices.

❒ If the syslog servers are not members of the same subnet as the management IP address of the switch, the switch must have a default gateway that specifies the first hop to reaching the servers. For instructions on specifying the default gateway, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The event messages are transmitted when they are generated. Any event messages that already exist in the event log are not transmitted when a new syslog server definition is created.

❒ The syslog client uses UDP port 514. You cannot change the UDP port.

Creating Syslog Server Definitions

To configure the switch to send event messages to a syslog server, create a syslog server definition with the LOG HOST command in the Global Configuration mode. Here is the format of the command:

```
log host ipaddress [level level] [program program]
```

This command creates just one definition at a time.

The IPADDRESS parameter is the IP address of a syslog server you want to receive event messages. You can specify just one address.

The LEVEL parameter specifies the minimal severity level of the events to transmit to the server. The switch supports the four severity levels in Table 55. Messages of the specified level and all levels below it are transmitted to the server. For example, specifying level 4 for a syslog server definition causes the switch to transmit levels 0 and 4 messages. If you omit this parameter, messages of all severity levels are sent.

Table 55. Event Message Severity Levels

Value	Severity Level	Description
0	Emergency	Switch operation is severely impaired.
4	Warning	An issue may require manager attention.
6	Informational	Useful information that can be ignored during normal operation.
7	Debug	Messages intended for technical support and software development.

The PROGRAM parameter is used to restrict the transmitted messages to just those that are generated by particular programs on the switch. You designate the programs by entering their abbreviations, listed in Table 56.

Table 56. Program Abbreviations

Abbreviation	Program
ALL	All features
ACL	Port access control list
CFG	Switch configuration
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands

Table 56. Program Abbreviations

Abbreviation	Program
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	System IP configuration
LACP	Link Aggregation Control Protocol
LLDP	LLDP and LLDP-MED
MAC	MAC address table
PACCESS	802.1x port-based access control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	MAC address-based port security
PTRUNK	Static port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RRP	RRP snooping
RTC	Real time clock
SFLOW	sFlow client
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; manager and operator log in and log off events.

Table 56. Program Abbreviations

Abbreviation	Program
TACACS	TACACS+ authentication protocol
TELNET	Telnet
TFTP	TFTP
TIME	System time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes
WATCHDOG	Watchdog timer

This example of the command creates a new syslog definition for a syslog server that has the IP address 149.24.111.23. The definition sends all event messages to the designated server.

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 149.24.111.23
```

This example creates a syslog definition that sends all messages with severity levels 0, 4 to a syslog server that has the IP address 122.34.152.165:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 122.34.152.165 level 4
```

This example creates a syslog definition that sends messages from the RADIUS, spanning tree protocols, and static port trunks, to a syslog server that has the IP address 156.74.134.76:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 156.74.134.76 program radius,stp,
ptrunk
```

This example creates a syslog definition that sends messages with severity levels 0, 4, and 6 from access control lists and MAC address-based port security, to a syslog server that has the IP address 118.87.45.72:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 118.87.45.72 level 6 program acl,
psec
```

533

Deleting Syslog Server Definitions

To delete syslog server definitions from the switch, use the NO LOG HOST command in the Global Configuration mode. The format of the command is:

no log host *ipaddress*

To view the IP addresses of the syslog servers of the definitions, use the SHOW LOG CONFIG command. You can delete just one definition at a time with this command.

The switch stops sending event messages to a syslog server as soon as you delete a definition.

This example deletes a syslog server definition for the server IP address 124.145.112.61:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log host 124.145.112.61
```

Displaying the Syslog Server Definitions

To view the IP addresses of the syslog servers use the SHOW LOG CONFIG command in the Privileged Exec mode:

```
awplus# show log config
```

Here is an example of the information.

```
Permanent log:
 Status ................ Enable
   Filter:
   Level .............. Informational
   Program ............ All
   Message Text .......
 Host 149.132.45.75:
   Filter:
   Level .............. Informational
   Program ............ All
   Message Text .......
 Host 149.132.101.128:
   Filter:
   Level .............. Informational
   Program ............ All
   Message Text .......
 Buffered log:
 Status ................ Enable
   Filter:
   Level .............. Informational
   Program ............ All
   Message Text .......
```

Figure 97. SHOW LOG CONFIG Command with Syslog Server Entries

The syslog server entries are marked with "Host," followed by the server IP addresses. The example display has two syslog server entries that have the IP addresses 149.132.45.75 and 149.132.101.128.

535

Chapter 35

Syslog Client Commands

The syslog client commands are summarized in Table 57 and described in detail within the chapter.

Table 57. Syslog Client Commands

Command	Mode	Description
"LOG HOST" on page 538	Global Configuration	Creates syslog server definitions.
"NO LOG HOST" on page 540	Global Configuration	Deletes syslog server definitions.
"SHOW LOG CONFIG" on page 541	Privileged Exec	Displays the syslog server definitions.

LOG HOST

Syntax

```
log host ipaddress [level level] [program program]
```

Parameters

ipaddress

Specifies the IP address of a syslog server. You can specify one address.

level

Specifies the minimum severity level of the messages to be sent to the designated syslog server. The severity levels are listed in Table 55 on page 531. You can specify only one severity level. Omit this parameter to send messages of severity levels 0, 4, and 6.

program

Specifies that only messages generated by particular management software modules are sent to the syslog server. The modules are listed in Table 53 on page 522. You can specify more than one feature. Separate multiple features with commas. Omit this parameter to send messages from all features.

Mode

Global Configuration mode

Description

Use this command to create syslog server definitions. The switch uses the definitions to send event messages to syslog servers on your network. There can be up to 19 syslog server definitions. You can create only one definition at a time with this command.

Confirmation Commands

"SHOW LOG CONFIG" on page 541

Examples

This example creates a new syslog definition that sends all event messages to a syslog server with the IP address 149.24.111.23:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 149.24.111.23
```

538

This example creates a new syslog definition for a syslog server that has the IP address 149.152.122.143. The definition sends only those messages that have a minimum severity level of 4 and that are generated by the RADIUS client (RADIUS) and static port trunks (PTRUNK):

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 149.152.122.143 level 4 program
radius,ptrunk
```

NO LOG HOST

Syntax

```
no log host ipaddress
```

Parameters

ipaddress
    Specifies an IP address of a syslog server.

Mode

Global Configuration mode

Description

Use this command to delete syslog server definitions from the switch.

Confirmation Command

"SHOW LOG CONFIG" on page 541

Example

This example deletes a syslog server definition with the server IP address 149.122.45.78:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log host 149.122.45.78
```

SHOW LOG CONFIG

Syntax

```
show log config
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the syslog server definitions on the switch. Here is an example of the information.

Figure 98 is an example of the information displayed.

```
Permanent log:
 Status ................ Enable
    Filter:
    Level ............. Informational
    Program ............ All
    Message Text .......
 Host 149.132.45.75:
    Filter:
    Level ............. Informational
    Program ............ All
    Message Text .......
 Host 149.132.101.128:
    Filter:
    Level ............. Informational
    Program ............ All
    Message Text .......
 Buffered log:
 Status ................ Enable
    Filter:
    Level ............. Informational
    Program ............ All
    Message Text .......
```

Figure 98 SHOW LOG CONFIG Command with Syslog Server Entries

The syslog server entries are marked with "Host," followed by the server IP addresses. The example display has two syslog server entries that have the IP addresses 149.132.45.75 and 149.132.101.128.

Example

This example displays the configurations of the syslog server entries:

```
awplus# show log config
```

Section V
Port Trunks

This section contains the following chapters:

544

Chapter 36

Static Port Trunks

This chapter covers the following topics:

Overview

Static port trunks are groups of two to eight ports that act as single virtual links between the switch and other network devices. Static port trunks are commonly used to improve network performance by increasing the available bandwidth between the switch and other network devices and to enhance the reliability of the connections between network devices.

Figure 99 is an example of a static port trunk of four links between two AT-9000 Switches.
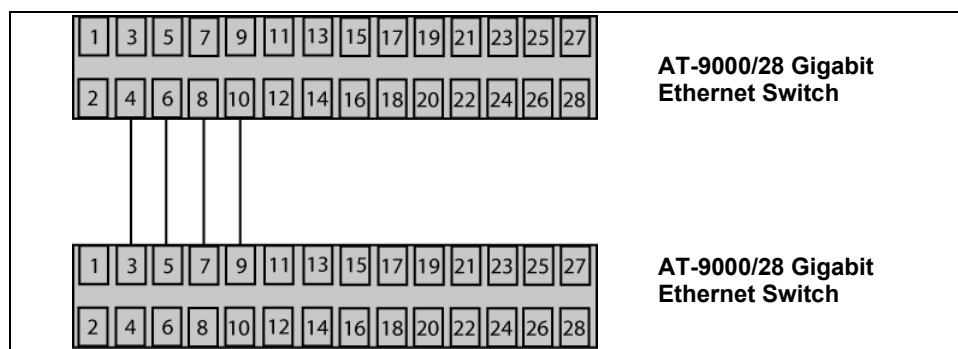
Figure 99. Static Port Trunk Example

When you create a new static port trunk, you can designate the manner in which the traffic is distributed across the physical links by the switch. This is explained in "Load Distribution Methods," next.

Unlike LACP trunks, which are described in Chapter 38, "Link Aggregation Control Protocol (LACP)" on page 563, static port trunks do not permit standby ports. If a link is lost on a port in a static port trunk, the trunk's total bandwidth is reduced. Although the traffic carried by a lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until a lost link is reestablished or another port is manually added to the trunk.

Load Distribution Methods

This section discusses the load distribution methods for static port trunks and LACP trunks, described in Chapter 38, "Link Aggregation Control Protocol (LACP)" on page 563.

When you create a static port trunk or an LACP trunk, you have to specify the manner in which the switch should distribute the packets of the traffic load across the ports of a trunk. This is referred to as the load distribution method. The load distribution methods are listed here:

- ❒ Source MAC Address (Layer 2)
- ❒ Destination MAC Address (Layer 2)

546

❏ Source MAC Address / Destination MAC Address (Layer 2)

❏ Source IP Address (Layer 3)

❏ Destination IP Address (Layer 3)

❏ Source IP Address / Destination IP Address (Layer 3)

The load distribution methods examine the last three bits of a packet's MAC or IP address and compare the bits against mappings assigned to the ports in the trunk. The port mapped to the matching bits is selected as the transmission port for a packet.

In cases where you select a load distribution that employs either a source or destination address but not both, only the last three bits of the designated address are used in the selection process. If you select one of the two load distribution methods employing both source and destination addresses, port selection is achieved through an XOR operation of the last three bits of both addresses.

For example, assume you created a static port trunk or an LACP trunk of Ports 7 through 14 on the switch. The table below shows the mappings of the switch ports to the possible values of the last three bits of a MAC or IP address.

Last 3 Bits	000 (0)	001 (1)	010 (2)	011 (3)	100 (4)	101 (5)	110 (6)	111 (7)
Trunk Ports	7	8	9	10	11	12	13	14

Assume you selected source MAC address as the load distribution method and that the switch needed to transmit over the trunk a packet with a source MAC address that ended in 9. The binary equivalent of 9 is 1001, making the last three bits of the address 001. An examination of the table above indicates that the switch uses Port 8 to transmit the frame because that port is mapped to the matching bits.

A similar method is used for the two load distribution methods that employ both the source and destination addresses. Only here the last three bits of both addresses are combined by an XOR process to derive a single value which is then compared against the mappings of the bits to ports. The XOR rules are as follows:

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

For example, assume you selected source and destination MAC addresses for the load distribution method in our previous example, and that a packet for transmission over the trunk had a source MAC address that ended in 9 and a destination address that ended in 3. The binary values are:

9 = 1001
3 = 0011

Applying the XOR rules above on the last three bits result in 010, or 2. An examination of the table above shows that the packet is transmitted from port 9.

Port trunk mappings on the switch can consist of up to eight ports. This corresponds to the maximum number of ports allowed in a static trunk and the maximum number of active ports in an LACP trunk. Inactive ports in an LACP trunk are not applied to the mappings until they transition to the active status.

You can assign different load distribution methods to different static trunks on the same switch. The same is true for LACP aggregators. However, it should be noted that all aggregate trunks within an LACP aggregator must use the same load distribution method.

The load distribution methods assume that the final three bits of the source and/or destination addresses of the packets from the network nodes are varied enough to support efficient distribution of the packets over the trunk ports. A lack of variation can result in one or more ports in a trunk being used more than others, with the potential loss of a trunk's efficiency and performance.

Guidelines

Here are the guidelines to using static port trunks:

- A static trunk can have up to eight ports.
- The switch supports up to a total of 32 static port trunks and LACP trunks at a time. An LACP trunk is counted against the maximum number of trunks when it is active.
- The ports of a static port trunk can be either all twisted pair ports or all fiber optic ports. Static port trunks cannot have both types of ports.
- The ports of a trunk can be either consecutive (for example ports 5-9) or nonconsecutive (for example, ports 4, 8, 11, 20).
- The ports of static port trunks must be from the same switch.
- Static port trunks are compatible with spanning tree protocols because the switch views them as single virtual links.
- Before creating a port trunk, examine the speed, duplex mode, flow control, and back pressure settings of the lowest number port the trunk will contain. Verify that these port configuration settings

are compatible with the device to which the trunk will be connected. When you create a static port trunk, the management software copies the current settings of the lowest numbered port in the trunk to the other ports, so that all the ports have the same settings. For example, if you create a port trunk of ports 5 to 8, the parameter settings for port 5 are copied to ports 6, 7, and 8 so that all the ports of the trunk have the same settings.

❐ After creating a port trunk, do not change the speed, duplex mode, flow control, or back pressure of any port in the trunk without also changing the other ports.

❐ A port can belong to only one static trunk at a time.

❐ A port cannot be a member of a static trunk and an LACP trunk at the same time.

❐ The ports of a static trunk must be untagged members of the same VLAN. A trunk cannot consist of untagged ports from different VLANs.

❐ The switch selects the lowest-numbered port in the trunk to handle broadcast packets and packets of an unknown destination. For example, a trunk of ports 11 to 15 uses port 11 for broadcast packets.

❐ Because network equipment vendors tend to employ different techniques for static trunks, a static trunk on one device might not be compatible with the same feature on a device from a different manufacturer. For this reason, Allied Telesis recommends using this feature only between Allied Telesis network devices.

Creating New Static Port Trunks or Adding Ports To Existing Trunks

The command to create new static port trunks or to add ports to existing trunks is the STATIC-CHANNEL-GROUP command. Here is the format of the command:

```
static-channel-group id_number
```

You perform the command from the Port Interface mode of the ports the trunk is to contain. Here is an example that creates a new trunk of ports 22 to 23 and the ID number 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22-port1.0.23
awplus(config-if)# static-channel-group 1
```

If a static port trunk of that ID number already exists, the commands add ports 22 and 23 to it.

⚠️ **Caution**

To prevent the formation of loops in your network topology, do not connect the network cables to the member ports of a trunk until after you have created it. Network loops can result in broadcast storms that can adversely affect network performance.

For reference information, refer to "STATIC-CHANNEL-GROUP" on page 560.

Specifying the Load Distribution Method

The load distribution method defines how the switch distributes the traffic among the ports of a trunk. The command for this is the PORT-CHANNEL LOAD-BALANCE command, in the Static Port Trunk Interface mode. The command's format is shown here:

```
port-channel load-balance dst-ip|dst-mac|src-dst-ip|
src-dst-mac|src-ip|src-mac
```

The variables are defined here:

src-mac   Specifies source MAC address as the load distribution method.

dst-mac   Specifies destination MAC address.

src-dst-mac   Specifies source address/destination MAC address.

src-ip   Specifies source IP address.

dst-ip   Specifies destination IP address.

src-dst-ip   Specifies source address/destination IP address.

To enter the Static Port Trunk Interface mode, you use the INTERFACE TRUNK command. You enter the INTERFACE keyword followed by the name of the trunk. The name of the trunk consists of the prefix "sa" (for static trunk) and the trunk's ID number. (If you do not know the ID number of the trunk, refer to "Displaying Static Port Trunks" on page 553.)

This example sets the load distribution method to destination MAC address for a static port trunk that has the ID number 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface sa4
awplus(config-if)# port-channel load-balance dst-mac
```

For reference information, refer to "PORT-CHANNEL LOAD-BALANCE" on page 557.

Removing Ports from Static Port Trunks or Deleting Trunks

To remove ports from a static port trunk, enter the Port Interface mode of the ports to be removed and issue the NO STATIC-CHANNEL-GROUP command. This example removes ports 4 and 5 from their current static port trunk assignment:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.5
awplus(config-if)# no static-channel-group
```

To delete a static port trunk, remove all its member ports. This example deletes a trunk that consists of member ports 15 to 17 and 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15-port1.0.17,port1.0.21
awplus(config-if)# no static-channel-group
```

Caution

To prevent the formation of loops in your network topology, do not remove ports from a static port trunk without first disconnecting their network cable. Network loops can result in broadcast storms that can adversely affect network performance.

Displaying Static Port Trunks

To display the member ports of static port trunks, use the SHOW STATIC-CHANNEL-GROUP command in the User Exec mode or Privileged Exec mode:

awplus# show static-channel-group

Here is an example of the information.

```
% Static Aggregator: sa1
% Member:
   port1.0.5
   port1.0.6
   port1.0.7
% Static Aggregator: sa2
% Member:
   port1.0.19
   port1.0.20
   port1.0.21
   port1.0.22
```

Figure 100. SHOW STATIC-CHANNEL-GROUP Command

To view the load distribution methods of static port trunks, display the running configuration with "SHOW RUNNING-CONFIG" on page 158.

553

Chapter 37

Static Port Trunk Commands

The static port trunk commands are summarized in Table 58 and described in detail within the chapter.

Table 58. Static Port Trunk Commands

Command	Mode	Description
"NO STATIC-CHANNEL-GROUP" on page 556	Port Interface	Removes ports from existing static port trunks and deletes trunks from the switch.
"PORT-CHANNEL LOAD-BALANCE" on page 557	Static Port Trunk Interface	Sets the load distribution methods of static port trunks.
"SHOW STATIC-CHANNEL-GROUP" on page 559	User Exec and Privileged Exec	Displays the specifications of the static port trunks.
"STATIC-CHANNEL-GROUP" on page 560	Port Interface	Creates a new static port trunk and adds ports to an existing static port trunk.

NO STATIC-CHANNEL-GROUP

Syntax

```
no static-channel-group
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove ports from static port trunks and to delete trunks. To delete a trunk, remove all its ports.

> ⚠️ **Caution**
> To prevent the formation of loops in your network topology, do not remove ports from a static port trunk without first disconnecting their network cable. Network loops can result in broadcast storms that can adversely affect network performance.

> **Note**
> You cannot leave a trunk with just one port. There must be a minimum of two ports in a trunk.

Example

These commands remove ports 22 and 23 from a static port trunk. If these are the only ports in the trunk, the trunk is deleted from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22-port1.0.23
awplus(config-if)# no static-channel-group
```

PORT-CHANNEL LOAD-BALANCE

Syntax

```
port-channel load-balance src-mac|dst-mac|src-dst-mac|src-
ip|dst-ip|src-dst-ip
```

Parameters

src-mac

Specifies source MAC address as the load distribution method.

dst-mac

Specifies destination MAC address.

src-dst-mac

Specifies source address/destination MAC address.

src-ip

Specifies source IP address.

dst-ip

Specifies destination IP address.

src-dst-ip

Specifies source address/destination IP address.

Mode

Static Port Trunk Interface mode

Description

Use this command to specify the load distribution methods of static port trunks. The load distribution methods determine the manner in which the switch distributes packets among the ports of a trunk.

This command is found in the Static Port Trunk Interface mode. To enter the mode, use the INTERFACE TRUNK command. The format of the command is the keyword INTERFACE followed by name of a trunk you want to configure. The name of a static port truck consists of "sa" followed by a trunk's ID number. You can configure just one trunk at a time.

Example

This example sets the load distribution method to destination MAC address for a trunk with an ID number 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface sa4
awplus(config-if)# port-channel load-balance dst-mac
```

558

SHOW STATIC-CHANNEL-GROUP

Syntax

show static-channel-group

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display the member ports of static port trunks on the switch. An example of the command is shown in Figure 101.

```
% Static Aggregator: sa1
% Member:
    port1.0.5
    port1.0.6
    port1.0.7
% Static Aggregator: sa2
% Member:
    port1.0.19
    port1.0.20
    port1.0.21
    port1.0.22
```

Figure 101. SHOW STATIC-CHANNEL-GROUP Command

To view the load distribution methods of static port trunks, display the running configuration with "SHOW RUNNING-CONFIG" on page 158.

Example

This example displays the member ports of a static port trunk:

awplus# show static-channel-group

STATIC-CHANNEL-GROUP

Syntax

```
static-channel-group id_number
```

Parameters

id_number
> Specifies an ID number of a static port trunk. The range is 1 to 32. You can specify just one ID number.

Mode

Port Interface mode

Description

Use this command to create new static port trunks and to add ports to existing trunks. To create a new trunk, specify an unused ID number. To add ports to an existing trunk, specify an ID number of an existing trunk.

⚠️ **Caution**
Do not connect the network cables to the ports of the static port trunk until after you have created it. A network loop may result if you connect the cables beforehand, possibly resulting in a broadcast storm and poor network performance.

To create a new static port trunk, you have to assign it an ID number, in the range of 1 to 32. This number is used by the switch to identify trunks and to assign trunk names. A name of a trunk consists of the prefix "sa" followed by an ID number. For instance, if you assign a new trunk the ID number 5, its name will be "sa5."

You should review the following information before creating a new static port trunk:

❒ When you create a new trunk, the settings of the lowest numbered port are copied to the other ports so that all the ports have the same settings. Consequently, you should examine and verify that the speed, duplex mode, and flow control settings of the lowest numbered port are correct for the network device to which the trunk will be connected.

❒ The ports of a trunk must be members of the same VLAN.

560

❑ Ports can be members of just one static port trunk at a time. A port that is already a member of a trunk cannot be added to another trunk until it is first removed from its current trunk assignment. To remove ports from static port trunks, see "NO STATIC-CHANNEL-GROUP" on page 556.

❑ Allied Telesis does not recommend using twisted pair ports 25R to 28R on the AT-9000/28 and AT-9000/28SP Managed Layer 2 ecoSwitches in static port trunks. The performance of a static port trunk that has these ports may not be predictable if the ports transition to the redundant state.

You should review the following information if you are adding ports to an existing trunk:

❑ If the port you are adding will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you check to see if its settings are appropriate prior to adding it to the trunk. If the port will not be the lowest numbered port, its settings are changed to match the settings of the existing ports in the trunk.

❑ If the port to be added to a trunk is already a member of another static trunk, you must first remove it from its current trunk assignment. To remove ports from a trunk, see "NO STATIC-CHANNEL-GROUP" on page 556.

Example

This example creates a new static port trunk of ports 11 and 12, with the ID number 2. If there is already a static port trunk with the same ID number the commands add the ports to it:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.12
awplus(config-if)# static-channel-group 2
```

561

Chapter 38

Link Aggregation Control Protocol (LACP)

This chapter covers the following topics:

Overview

The Link Aggregation Control Protocol (LACP) is used to increase the bandwidth between the switch and other LACP-compatible devices by grouping ports together to form single virtual links.

LACP trunks are similar in function to static port trunks, but they are more flexible. The implementations of static trunks tend to be vendor specific and so may not always be compatible. In contrast, the implementation of LACP in the switch is compliant with the IEEE 802.3ad standard. It is interoperable with equipment from other vendors that also comply with the standard. This makes it possible to create LACP trunks between the switch and network devices from other manufacturers.

The main component of an LACP trunk is an aggregator. An aggregator is a group of ports on the switch. The ports of an aggregator are further grouped into a trunk, referred to as an aggregate trunk. An aggregate trunk can consist of a maximum of 8 ports on the switch.

An aggregator can have only one trunk. You have to create a separate aggregator for each trunk on the switch. The switch up can support up to a total of 32 static and LACP aggregate trunks at a time

LACP System Priority

When two devices form an aggregate trunk, a conflict may occur if there is a difference in their LACP implementations. For example, the two devices might not support the same number of active ports in an aggregate trunk.

If a conflict does occur, the two devices must resolve the problem and decide whose LACP settings take precedence. This is accomplished with the system LACP priority value. A hexadecimal value of from 1 to FFFF, this parameter is used whenever the devices encounter a conflict creating a trunk. The lower the number, the higher the priority. The settings on the device with the higher priority take precedence over the settings on the other device. If both devices have the same system LACP priority value, the settings on whichever switch has the lowest MAC address takes precedence.

This parameter is useful if the switch and the other 802.3ad-compliant device have different LACP trunking capabilities. You should give the other device the higher priority if its LACP capability is less than the AT-9000 Series switch capability. That way, the other device's settings are used by both devices to form the trunk.

For example, a conflict could occur in an aggregate trunk of six links if the other 802.3ad-compliant device supported just four active links at one time. The AT-9000 Series switch would activate all six links, while the other device would activate only four ports. But by giving the other device the higher priority, the conflict is avoided because the AT-9000 Series switch would use only four active links.

564

Base Port
The lowest numbered port in an aggregator is referred to as the base port. You cannot change the base port of an aggregator. You can neither delete it from an aggregator nor add any ports that are below it. For example, if an aggregator consists of ports 5 to 12, you cannot delete port 5 because it is the base port, and you are not allowed to add ports 1 to 4 to the aggregator. If you need to change the base port of an aggregator, you must delete and recreate the aggregator to which it belongs.

Load Distribution Methods
The load distribution method determines the manner in which the switch distributes the traffic across the active ports of an aggregate trunk. The method is assigned to an aggregator and applies to the aggregate trunk in it. For further information, refer to "Load Distribution Methods" on page 546.

Guidelines
Here are the LACP guidelines:

- □ LACP must be activated on both the switch and the other device.
- □ The other device must be 802.3ad-compliant.
- □ An aggregator can consist of any number of ports.
- □ The switch supports up to eight active ports in an aggregate trunk at a time.
- □ The switch can support up to a total of 32 static and LACP aggregate trunks at a time. An LACP trunk is countered against the maximum number of trunks only when it is active.
- □ The ports of an aggregate trunk must be the same medium type: all twisted pair ports or all fiber optic ports.
- □ The ports of a trunk can be consecutive (for example ports 5 to 9) or nonconsecutive (for example, ports 4, 8, 11, 20).
- □ A port can belong to only one aggregator at a time.
- □ A port cannot be a member of an aggregator and a static trunk at the same time.
- □ The ports of an aggregate trunk must be untagged members of the same VLAN.
- □ 10/100/1000Base-TX twisted pair ports must be set to Auto-Negotiation or 100 Mbps, full-duplex mode. LACP trunks are not supported in half-duplex mode.
- □ 100Base-FX fiber optic ports must be set to full-duplex mode.
- □ You can create an aggregate trunk of SFP transceivers in the AT-9000/52 Switch.
- □ Only those ports that are members of an aggregator transmit LACPDU packets.
- □ Combo ports of all AT-9000 models can be aggregated, but not combined with any base ports.

❐ The lowest numbered port in an aggregator is called the base port. You cannot add ports that are below the base port of an aggregator. For example, you cannot add ports 1 to 3 to an aggregator that consists of ports 4 to 8. You must delete and recreate an aggregator to change its base port.

❐ The load distribution method is applied at the aggregator level. For further information, refer to "Load Distribution Methods" on page 546.

❐ To function as a member of an aggregator, a port must receive LACPDU packets from a remote network device. A port that does not receive LACPDU packets while it is a member of an aggregate trunk functions as a regular Ethernet port, forwarding network traffic while also continuing to transmit LACPDU packets.

❐ The port with the highest priority in an aggregate trunk carries broadcast packets and packets with an unknown destination.

❐ Prior to creating an aggregate trunk between an Allied Telesis device and another vendor's device, refer to the vendor's documentation to determine the maximum number of active ports the device supports. If the number is less than eight, the maximum number for the AT-9000 Series switch, you should assign the vendor's device a higher system LACP priority than the switch. If it is more than eight, assign the AT-9000 Series switch the higher priority. This will avoid a possible conflict between the devices if some ports are placed in the standby mode when the devices create the trunk. For background information, refer to "LACP System Priority" on page 564.

❐ LACPDU packets are transmitted as untagged packets.

Creating New Aggregators

To create a new aggregator, move to the Port Interface mode of the aggregator's member ports and issue the CHANNEL-GROUP command, which has this format:

channel-group *id_number*

The ID_NUMBER parameter has a range of 1 to 32. Each aggregator must be assigned a unique ID number.

If the ports of a new aggregator are already members of other aggregators, the switch automatically removes them from their current assignments before adding them to the new aggregator.

⚠️ **Caution**

To avoid creating a loop in your network topology, do not connect the network cables to the ports until after you have created the aggregator with the CHANNEL-GROUP command.

These commands create a new aggregator of ports 11 and 12, with the ID number 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.12
awplus(config-if)# channel-group 4
```

Setting the Load Distribution Method

The load distribution method determines the manner in which the switch distributes the egress packets among the active ports of an aggregator. The packets can be distributed by source MAC or IP address, destination MAC or IP address, or by both source and destination addresses. The distribution methods are discussed in "Load Distribution Methods" on page 546.

The load distribution method of an aggregator is set with the PORT-CHANNEL LOAD-BALANCE command in the LACP Port Trunk Interface mode. To enter the mode, use the INTERFACE PO command from the Global Configuration mode, in this format:

```
interface po id_number
```

You specify the intended aggregator by adding its ID number as a suffix to PO.

Here is the format of the PORT-CHANNEL LOAD-BALANCE command:

```
port-channel load-balance src-mac|dst-mac|src-dst-mac|
src-ip|dst-ip|src-dst-ip
```

In this example, an aggregator with the ID number 5 is assigned the source MAC address distribution method:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface po5
awplus(config-if)# port-channel load-balance src-mac
```

This example assigns an aggregator with the ID number 17 the source destination MAC address distribution method:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface po17
awplus(config-if)# port-channel load-balance src-dst-mac
```

Adding Ports to Aggregators

The command to add ports to existing aggregators is the same command to create new aggregators, the CHANNEL-GROUP command in the Port Interface mode. To use the command, move to the Port Interface mode of the ports you want to add to an aggregator and issue the command.

Note
You cannot add to an aggregator any ports that are below the base port. For instance, you cannot add any ports below port 15 to an aggregator that has ports 15 to 22.

When you enter the command, specify the ID number of the existing aggregator to which the new ports are to be assigned. If you do not know the ID number, use the SHOW ETHERCHANNEL DETAIL command.

If the new ports of an aggregator are already members of other aggregators, you do not have to remove them from their current assignments before adding them to a different aggregator. The management software does that automatically.

⚠️ **Caution**
To avoid creating a loop in your network topology, do not connect the network cables to the aggregator ports until you have performed the CHANNEL-GROUP command.

These commands add ports 18 and 23 to the aggregator with ID number 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.23
awplus(config-if)# channel-group 5
```

Removing Ports from Aggregators

To remove ports from an aggregator, use the NO CHANNEL-GROUP command, in the Port Interface mode. Move to the Port Interface mode for those ports you want to remove from an aggregator and enter the command. You can remove ports from only one aggregator at a time.

⚠️ **Caution**

Do not remove a port from an aggregator without first disconnecting the network cable. Leaving the network cable connected may result in a network loop, which can cause a broadcast storm.

Note

You cannot remove the base port of an aggregator. The base port is the lowest-numbered port of an aggregator. For example, you cannot delete port 7 from an aggregator consisting of ports 7 to 12. Removing the base port requires deleting and recreating the aggregator to which the base port belongs.

These commands delete ports 11 and 12 from an aggregator:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.12
awplus(config-if)# no channel-group
```

Deleting Aggregators

To delete an aggregator, remove all its ports with the NO CHANNEL-GROUP command, in the Port Interface mode.

> ⚠️ **Caution**
>
> Do not delete an aggregator without first disconnecting the network cables from its ports. Leaving the network cables connected may result in a network loop, which can cause a broadcast storm.

These commands delete an aggregator consisting of ports 17, 22 and 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17,port1.0.22,port1.0.23
awplus(config-if)# no channel-group
```

Displaying Aggregators

There are five SHOW commands for LACP. Two of them are mentioned here. For descriptions of all the commands, refer to Chapter 39, "LACP Commands" on page 575.

The first command is the SHOW ETHERCHANNEL DETAIL command in the Privileged Exec mode. It displays configuration information and operation status about the aggregators on the switch. Included are the ports of the individual aggregators, their link states, and the load distribution methods of the aggregators. Here is the command:

```
awplus# show etherchannel detail
```

Here is an example of the information.
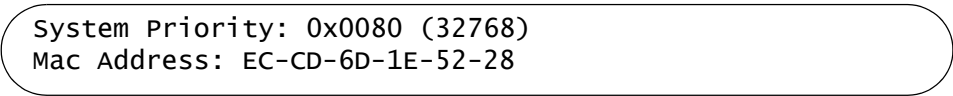
```
Aggregator # 1 ..... po1

Mac address: (00-15-77-d8-43-60,0000)
Admin Key: 0xff01 - Oper Key: 0x0101
Receive link count: 4 - Transmit link count: 4
Individual: 0 - Ready: 0
Distribution Mode .. MACBoth
Partner LAG: (0080,00-a0-d2-00-94-24,F601)
   Link: Port 1.0.1   sync
   Link: Port 1.0.2   sync
   Link: Port 1.0.3   sync
   Link: Port 1.0.4   sync

Aggregator # 22..... po22

Mac address: (00-15-77-d8-43-60,0000)
Admin Key: 0xff16 - Oper Key: 0x1616
Receive link count: 0 - Transmit link count: 0
Individual: 0 - Ready: 0
Distribution Mode .. MACDest
Partner LAG: (0000,00-00-00-00-00-00,0000)
   Link: Port 1.0.22  disabled
   Link: Port 1.0.23  disabled
   Link: Port 1.0.24  disabled
```

Figure 102. SHOW ETHERCHANNEL DETAIL

The only information the SHOW ETHERCHANNEL DETAIL command does not include is the LACP system priority value. That value can been seen with the SHOW LACP SYS-ID command, also in the Privileged Exec mode. Here is the command:

```
awplus# show lacp sys-id
```

Here is an example of the information.

```
System Priority: 0x0080 (32768)
Mac Address: EC-CD-6D-1E-52-28
```

Figure 103. SHOW LACP SYS-ID Command

It should be mentioned that while the system priority value is set as an integer with the LACP SYSTEM-PRIORITY command, this command displays it in hexadecimal format.

Chapter 39

LACP Commands

The LACP port trunk commands are summarized in Table 59 and described in detail within the chapter.

Table 59. LACP Port Trunk Commands

Command	Mode	Description
"CHANNEL-GROUP" on page 576	Port Interface	Creates new aggregators and adds ports to existing aggregators.
"LACP SYSTEM-PRIORITY" on page 578	Global Configuration	Sets the LACP system priority value for the switch.
"NO CHANNEL-GROUP" on page 579	Port Interface	Removes ports from aggregators and deletes aggregators.
"PORT-CHANNEL LOAD-BALANCE" on page 580	LACP Port Trunk Interface	Sets the load distribution method.
"SHOW ETHERCHANNEL" on page 582	Privileged Exec	Displays the ports of the aggregators on the switch.
"SHOW ETHERCHANNEL DETAIL" on page 583	Privileged Exec	Displays the states of the ports of the aggregators.
"SHOW ETHERCHANNEL SUMMARY" on page 585	Privileged Exec	Displays detailed information about the aggregators.
"SHOW LACP SYS-ID" on page 586	Privileged Exec	Displays the LACP priority value and MAC address of the switch.
"SHOW PORT ETHERCHANNEL" on page 587	Privileged Exec	Displays the LACP port information.

CHANNEL-GROUP

Syntax

channel-group *id_number*

Parameters

id_number

Specifies the ID number of a new or an existing aggregator. The range is 1 to 32.

Mode

Port Interface mode

Description

Use this command to create new aggregators or to add ports to existing aggregators.

The lowest numbered port in an aggregator is called the base port. When adding ports to an existing aggregator, you cannot add ports that are below the base port. For example, you cannot add ports 1 to 6 to an existing aggregator that consists of ports 7 to 12. You have to delete and recreate an aggregator to change its base port.

To review the guidelines to creating or modifying aggregators, refer to "Guidelines" on page 565.

⚠️ **Caution**

To prevent creating a loop in your network topology, do not connect the network cables to the ports until after you have created the aggregator. Network loops can cause broadcast storms that can lead to poor network performance.

Confirmation Command

"SHOW ETHERCHANNEL" on page 582

Examples

These commands create a new aggregator consisting of ports 11 to 16. The ID number of the aggregator is 2.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.16
awplus(config-if)# channel-group 2
```

This example adds port 15 to an existing aggregator that has the ID number 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# channel-group 4
```

LACP SYSTEM-PRIORITY

Syntax

```
lacp system-priority priority
```

Parameters

priority

Specifies the LACP system priority value for the switch. The range is 1 to 65535.

Mode

Global Configuration mode

Description

Use this command to set the LACP priority of the switch. The switch uses the LACP priority to resolve conflicts with other network devices when it creates aggregate trunks.

Confirmation Command

"SHOW LACP SYS-ID" on page 586

Note

The value is set as an integer with this command and displayed in hexadecimal format by the SHOW LACP SYS-ID command.

Example

This example assigns the system priority 200 to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# lacp system-priority 200
```

578

NO CHANNEL-GROUP

Syntax

```
no channel-group
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove ports from aggregators and to delete aggregators. To delete an aggregator, remove all its ports.

You cannot remove the base port of the aggregator. Changing the base port requires deleting and recreating the aggregator.

> ⚠️ **Caution**
> To prevent creating a loop in your network topology, you should not remove ports from an aggregator without first disconnecting their network cables. Network loops can cause broadcast storms that can lead to poor network performance.

Confirmation Command

"SHOW ETHERCHANNEL" on page 582

Example

These commands delete ports 11 and 12 from an aggregator. The aggregator is deleted if these are its only ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.12
awplus(config-if)# no channel-group
```

579

PORT-CHANNEL LOAD-BALANCE

Syntax

port-channel load-balance *src-mac|dst-mac|src-dst-mac|*
src-ip|dst-ip|src-dst-ip

Parameters

src-mac
> Specifies source MAC address as the load distribution method.

dst-mac
> Specifies destination MAC address.

src-dst-mac
> Specifies source address/destination MAC address.

src-ip
> Specifies source IP address.

dst-ip
> Specifies destination IP address.

src-dst-ip
> Specifies source address/destination IP address.

Mode

LACP Port Trunk Interface mode

Description

Use this command to set the load distribution methods of aggregators. An aggregator can have only one load distribution method. The load distribution methods are the same as those for static port trunks described in "Load Distribution Methods" on page 546.

To enter the LACP Port Trunk Interface mode, from the Global Configuration mode, enter the INTERFACE PO command and the ID number of the aggregator. For example, to enter the mode for the aggregator that has the ID number 2, you enter:

awplus> enable
awplus# configure terminal
awplus(config)# interface po2

580

Confirmation Command

"SHOW ETHERCHANNEL DETAIL" on page 583

Example

This example sets the load distribution method to source MAC address for the LACP trunk that has the ID number 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface po22
awplus(config-if)# port-channel load-balance src-mac
```

SHOW ETHERCHANNEL

Syntax

show etherchannel *id_number*

Parameters
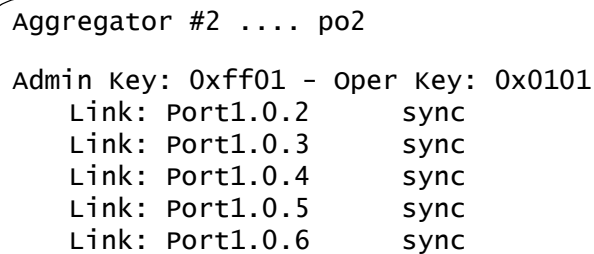
id_number
    Specifies the ID number of the aggregator.

Mode

Privileged Exec mode

Description

Use this command to display the ports of specific aggregators on the switch. Figure 104 illustrates the information.

```
Aggregator #2 .... po2

Admin Key: 0xff01 - Oper Key: 0x0101
    Link: Port1.0.2      sync
    Link: Port1.0.3      sync
    Link: Port1.0.4      sync
    Link: Port1.0.5      sync
    Link: Port1.0.6      sync
```

Figure 104. SHOW ETHERCHANNEL Command

Example

This example displays the ports of the aggregator with the ID number 22:

awplus# show etherchannel 22

582

SHOW ETHERCHANNEL DETAIL

Syntax

show etherchannel detail

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display detailed information about the aggregators on the switch. Figure 105 illustrates the information.

```
Aggregator # 1 ..... po1

 Mac address: (00-15-77-d8-43-60,0000)
 Admin Key: 0xff01 - Oper Key: 0x0101
 Receive link count: 4 - Transmit link count: 4
 Individual: 0 - Ready: 0
 Distribution Mode .. MACBoth
 Partner LAG: (0080,00-a0-d2-00-94-24,F601)
 Link: Port 1.0.1     sync
 Link: Port 1.0.2     sync
 Link: Port 1.0.3     sync
 Link: Port 1.0.4     sync

 Aggregator # 22..... po22

 Mac address: (00-15-77-d8-43-60,0000)
 Admin Key: 0xff16 - Oper Key: 0x1616
 Receive link count: 0 - Transmit link count: 0
 Individual: 0 - Ready: 0
 Distribution Mode .. MACDest
 Partner LAG: (0000,00-00-00-00-00-00,0000)
 Link: Port 1.0.22    disabled
 Link: Port 1.0.23    disabled
 Link: Port 1.0.24    disabled
```

Figure 105. SHOW ETHERCHANNEL DETAIL Command

Example

This example displays detailed information about aggregators:

```
awplus# show etherchannel detail
```

SHOW ETHERCHANNEL SUMMARY

Syntax

```
show etherchannel summary
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the states of the member ports of the aggregators. Figure 106 illustrates the information.

```
Aggregator #2 .... po2

Admin Key: 0xff01 - Oper Key: 0x0101
    Link: Port1.0.2      sync
    Link: Port1.0.3      sync
    Link: Port1.0.4      sync
    Link: Port1.0.5      sync
    Link: Port1.0.6      sync

Aggregator #21 .... po21

Admin Key: 0xff16 - Oper Key: 0x1616
    Link: Port1.0.21     disabled
    Link: Port1.0.22     disabled
    Link: Port1.0.23     disabled
    Link: Port1.0.24     disabled
    Link: Port1.0.25     disabled
```

Figure 106. SHOW ETHERCHANNEL SUMMARY Command

Example

This example displays the states of the aggregator's member ports:

```
awplus# show etherchannel summary
```

585

SHOW LACP SYS-ID

Syntax

```
show lacp sys-id
```

Parameters
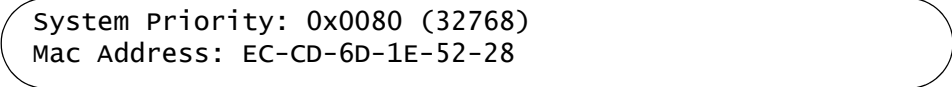
None

Mode

Privileged Exec mode

Description

Use this command to display the LACP priority value and MAC address of the switch. Figure 107 provides an example of the display.

```
System Priority: 0x0080 (32768)
Mac Address: EC-CD-6D-1E-52-28
```

Figure 107. SHOW LACP SYS-ID Command

Note
The LACP priority value is set as an integer with "LACP SYSTEM-PRIORITY" on page 578 and displayed in hexadecimal format by this command.

Example

This example displays the LACP priority value and MAC address:

```
awplus# show lacp sys-id
```

SHOW PORT ETHERCHANNEL

Syntax

```
show port etherchannel [interface port]
```

Parameters

port

Specifies the port of an aggregator. You can display more than one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display the LACP port information. Figure 108 illustrates the information. Refer to the IEEE 802.3ad standard for definitions of the fields.

```
Link: port: 1.0.5
Aggregator # 2
Receive machine state: Defaulted
Periodic Transmission machine state: Slow periodic
Mux machine state: Detached
ACTOR                              PARTNER
==========================================================================
Actor Port ............. 05        Partner Port ......... 00
Selected ............... UNSELECTED Partner System ....... 00-00-00-00-00-00
Oper Key ............... 0x0001    Oper Key  ............ 0x0000
Oper Port Priority  .... 0x0005    Oper Port Priority ... 0x0000
Individual ............. NO        Individual ........... YES
Synchronized........... NO         Synchronized.......... NO
Collecting  ........... NO         Collecting ........... NO
Distributing ........... NO        Distributing ......... NO
Defaulted .............. YES       Defaulted ............ NO
Expired ................ NO        Expired .............. NO
Actor Churn   .......... NO        Partner Churn ........ NO
```

Figure 108. SHOW PORT ETHERCHANNEL Command

Example

This example displays the LACP port information for port 5:

```
awplus# show port etherchannel port1.0.5
```

587

Section VI
Spanning Tree Protocols

This section contains the following chapters:

590

Chapter 40

STP, RSTP and MSTP Protocols

This chapter covers the following topics:

Overview

The Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. The problem that data loops pose is that packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.

Spanning tree prevents loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode.

Spanning tree can also activate redundant paths if primary paths go down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating backup redundant paths.

One of the primary differences between the two protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent lost of data packets.

RSTP is much faster and is the default spanning tree mode. It can complete a convergence in seconds to greatly diminish the possible impact the process can have on your network.

MSTP is similar to RSTP in its efficiency of convergence. It also allows more than one instance of spanning tree to be active at a time. See "Multiple Spanning Tree Protocol (MSTP)" on page 671 for more information about how MSTP operates in an environment of multiple spanning tree instances.

The STP implementation on the switch complies with the IEEE 802.1d standard. The RSTP implementation complies with the IEEE 802.1w standard. The MSTP feature complies with the IEEE 802.1s standard. The following subsections provide an overview the basic features of STP, RSTP and MSTP, and define the different parameters that you can adjust.

Bridge Priority and the Root Bridge

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by the *bridge priority* number, also referred to as the bridge identifier. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges, the one with the lowest MAC address is designated as the root bridge.

You can change the bridge priority number on the switch. You can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge offline, and assign that bridge the second lowest bridge identifier number.

The bridge priority has a range 0 to 61,440 in increments of 4,096. A lower priority number indicates a greater likelihood of the switch becoming the root bridge. The priority values can be set only in increments of 4,096. The default value is 32,768.

Path Costs and Port Costs

After the root bridge has been selected, the bridges determine if the network contains redundant paths and, if one is found, select a preferred path while placing the redundant paths in a backup or blocking state.

A bridge that has only one path between itself and the root bridge is referred to as the *designated bridge*. And the port through which it is communicating with the root bridge is referred to as the *root port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by a determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path, and the redundant paths are placed in the blocking state.

Path cost is determined by evaluating *port costs*. Every port on a bridge participating in STP and RSTP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is simply the sum of the port costs between a bridge and the root bridge.

The path cost of a port is adjustable on the switch. The range is 1 to 200000000.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter is used as a tie breaker when two paths have the same cost.

The port priority has a range from 0 to 240 in increments of 16. The priority values can be set only in increments of 16. The default value is 128, which is increment 8.

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all the bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporary data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states—listening and learning—before beginning to forward frames. The amount of time a port spends in these states is set by the forwarding delay value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the switch. The appropriate value for this parameter depends on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is needlessly delayed, which could result in the delay or loss of some data packets.

Note
The forwarding delay parameter applies only to ports on the switch that are operating STP-compatible mode.

Hello Time and Bridge Protocol Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the bridge protocol data unit (BPDU). When a bridge is brought online, it issues a BPDU in order to determine whether a root bridge has already been selected in the network, and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the hello time. This is a value that you can set on the switch. The interval is measured in seconds and has a default setting of two seconds. Consequently, if the switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

Part of the task of configuring RSTP or MSTP is defining the port types on the switch. This relates to the devices connected to the ports. With the port types defined, RSTP or MSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

Note
This section applies only to RSTP and MSTP.

There are two possible selections:

❑ Point-to-point port

❑ Edge port

A port that is operating in full-duplex mode is functioning as a point-to-point port. Figure 109 illustrates two switches that are connected with one data link. With the link operating in full-duplex, the ports are point-to-point ports.

Point to Point Ports
(Full Duplex Mode)
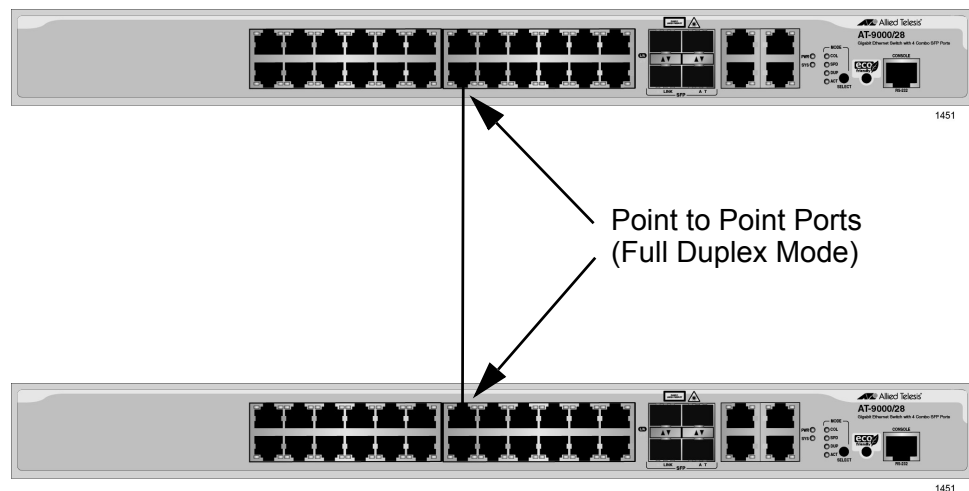
Figure 109. Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges that are participating in spanning tree, then the port is an edge port. Figure 110 on page 599 illustrates an edge port on the switch. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device that has no participating RSTP or MSTP devices.
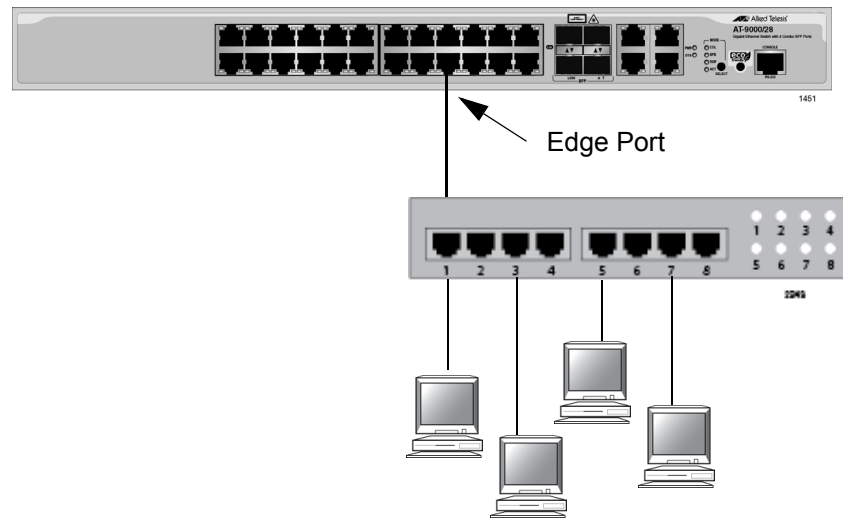
Figure 110. Edge Port

A port can be both a point-to-point and an edge port at the same time. It operates in full-duplex and has no spanning tree devices connected to it. Figure 111 illustrates a port functioning as both a point-to-point and edge port.
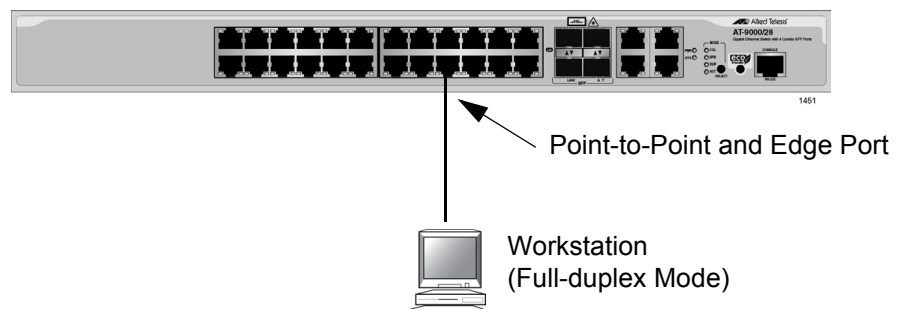
Figure 111. Point-to-Point and Edge Port

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason, do not change the default values for this RSTP feature unless you have a good grasp of the concept. In most cases, the default values work well.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. A network can have both protocols. If both RSTP and STP are present in a network, they operate together to create a single spanning tree domain. Given this, if you decide to activate spanning tree on the switch, there is no reason not to use RSTP, even if the other switches are running STP. The switch combines its RSTP with the STP on the other switches by monitoring the traffic on the ports for BPDU packets. Ports that receive RSTP BPDU packets operate in RSTP mode while ports receiving STP BPDU packets operate in STP mode.

Spanning Tree and VLANs

STP and RSTP support a single-instance spanning tree that encompasses all the ports on the switch. If the ports are divided into different VLANs, the spanning tree protocol crosses the VLAN boundaries. This point can pose a problem in networks that contain multiple VLANs that span different switches and that are connected with untagged ports. In this situation, STP and RSTP might block a data link if they detect a data loop, causing fragmentation of your VLANs.

This issue is illustrated in Figure 112. Two VLANs, Sales and Production, span two switches. Two links consisting of untagged ports connect the separate parts of each VLAN. If STP or RSTP is activated on the switches, one of the links is disabled because the links form a loop. In the example, the port on the top switch that links the two parts of the Production VLAN is changed to the block state. This leaves the two parts of the Production VLAN unable to communicate with each other.
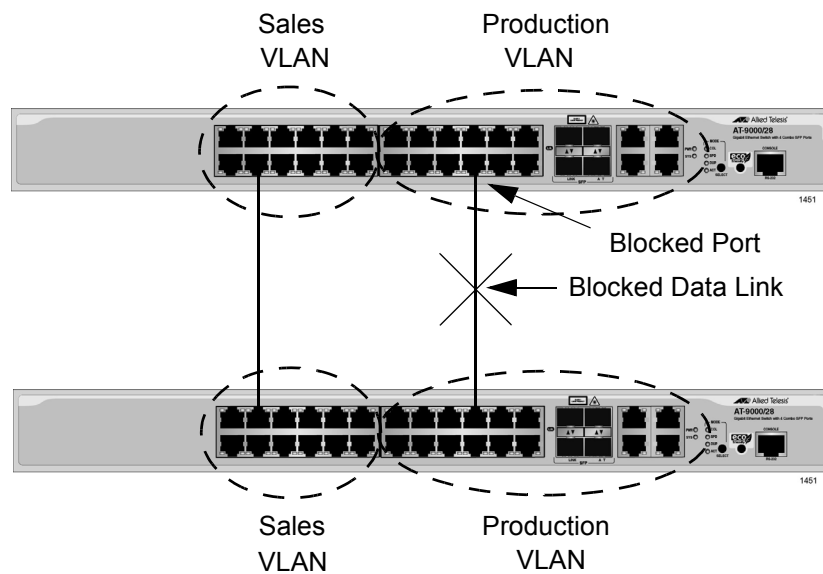
Figure 112. VLAN Fragmentation

You can avoid this problem by not activating spanning tree or by connecting VLANs using tagged instead of untagged ports. (For information about tagged and untagged ports, refer to Chapter 47, "Port-based and Tagged VLANs" on page 717.)

RSTP and MSTP BPDU Guard

This feature monitors the RSTP or MSTP edge ports on the switch for BPDU packets. Edge ports that receive BPDU packets are disabled by the switch. The benefit of this feature is that it prevents the use of edge ports by RSTP or MSTP devices. This reduces the possibility of unwanted changes to a network topology.

> **Note**
> This section applies only to RSTP and MSTP.

When RSTP or MSTP detects a loop in a network topology, it performs a process called convergence in which the spanning tree devices identify the ports to be blocked to prevent the loop. The length of time the process requires depends on a number of factors, including the number of devices and ports in the domain. Long convergence processes can affect network performance because areas of a network may be isolated while the devices check for loops and enable or disable ports.

You can decrease the amount of time of the convergence process by designating edge ports on the switches. These ports are connected to devices that are at the edge of a network, such as workstations and printers. The advantages of edge ports are that they typically do not participate in the convergence process and that they immediately transition to the forwarding state, skipping the intermediate listening and learning states.

Edge ports, however, can leave a spanning tree domain vulnerable to unwanted topology changes. This can happen if someone connects an RSTP or MSTP device to an edge port, causing the other devices in the domain to perform the convergence process to integrate the new device into the spanning tree domain. If the new device assumes the role of root bridge, the new topology might be undesirable. In the worst case scenario, someone could use an edge port to introduce false BPDUs into a network to deliberately initiate a change.

The BPDU guard feature lets you protect your network from unnecessary convergences by preventing the use of edge ports by RSTP or MSTP devices. When this feature is active on the switch, any edge port that receives BPDU packets is automatically disabled, preventing the initiation of the convergence process. You are notified of the event with an SNMP trap. An edge port remains disabled until you enable it again with the management software, such as with the ENABLE SWITCH PORT command in the command line.

Here are the guidelines to this feature:

❒ BPDU guard is configured for each port and has only two possible settings: enabled or disabled. The default setting is disabled.

❒ This feature is supported on the base ports of the switch and any fiber optic transceivers installed in the unit.

Note
A port disabled by the BPDU guard feature remains in that state until you enable it with the management software. If a port is still receiving BPDUs, you should disconnect the network cable before enabling it to prevent the feature from disabling the port again.

STP, RSTP, MSTP Loop Guard

Although spanning tree is designed to detect and prevent the formation of loops in a network topology, it is possible in certain circumstances for the protocol to inadvertently create loops. This can happen in the unlikely situation where a link between two spanning tree devices remains active when there is an cessation of BPDUs because of a hardware or software problem. The loop guard feature is designed to prevent the formation of loops in this situation.

> **Note**
> The Loop Guard feature is supported in STP, RSTP, and MSTP.

Network devices running spanning tree regularly transmit BPDUs to discover the topology of a network and to the search for loops. These packets are used by the devices to identify redundant physical paths to the root bridge and, where loops exist, to determine the ports to be blocked.

The proper operation of spanning tree relies on the flow of these packets. If there is a hardware or software failure that interrupts their transmission or reception, it is possible the protocol might mistakenly unblock one or more ports in the spanning tree domain, causing a network loop.

The loop guard feature protects against this type of failure by monitoring the ports on the switch for BPDUs from the other RSTP devices. If a port stops receiving BPDUs without a change to its link state (that is the link on a port stays up), the switch assumes that there is a problem with RSTP on the other device and takes action depending on a port's role in the spanning tree domain. If the event happens on an alternate port in the blocking state, the port is kept in that state. If this occurs on a root or designated port in the forwarding state, the port's state is changed to the blocking state.

The switch activates loop guard only when there is a cessation in the flow of BPDUs on a port whose link state has not changed. A port that never receives BPDUs will not be affected by this feature.

A port that loop guard has placed in the blocking state remains in that state until it begins to receive BPDUs again or you reset the switch. Disconnecting the port, disabling or enabling a port with the management software, or even disabling loop guard does not change a port's blocking state.

If a loop guard event occurs during a local or remote management session, you will see this message displayed on the screen:

```
Loop Guard is triggered
```

If you configured the SNMP community strings on the switch, an SNMP trap is sent to your management workstations to notify you of the event. However, this event does not generate an entry in the switch's log.

This feature is supported on the base ports of the switch as well as on any fiber optic transceivers installed in the unit.

The following figures illustrate this feature. The first figure shows spanning tree under normal operations in a network of three switches that have been connected to form a loop. To block the loop, switch 3 designates port 14 as an alternate port and places it in the blocking or discarding state.

Switch 2

Switch 1
Root bridge

Port 17
Forwarding state

Port 14
Blocking state
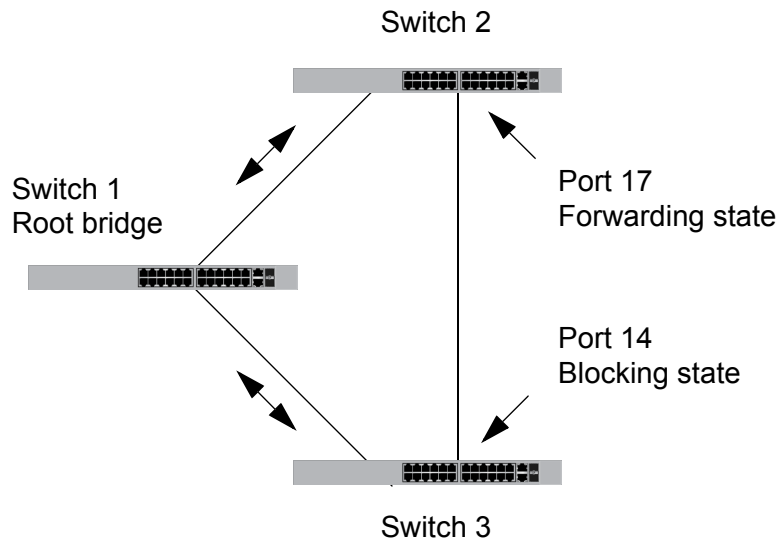
Switch 3

Figure 113. Loop Guard Example 1

If port 17 on switch 2 stops transmitting BPDUs, port 14 on switch 3 transitions from the blocking state to the forwarding state because the switch assumes that the device connected to the port is no longer an RSTP device. The result is a network loop, as illustrated in Figure 114 on page 606.

Switch 2

Switch 1
Root bridge

Port 17
Stops transmitting BDPUs

Port 14
Transitions to the forwarding
state from the blocking state
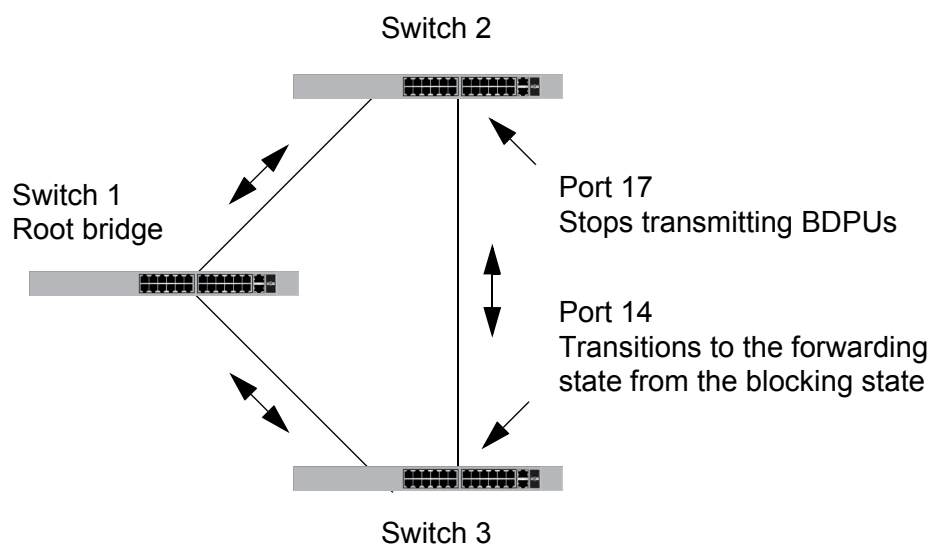
Switch 3

Figure 114. Loop Guard Example 2

But if loop guard is enabled on port 14 on switch 3, the port, instead of changing to the forwarding state, stays in the blocking state, preventing the formation of the loop.

Switch 2

Switch 1
Root bridge

Port 17
Stops transmitting BPDUs

Port 14
Loop guard keeps the port
in the blocking state

Switch 3
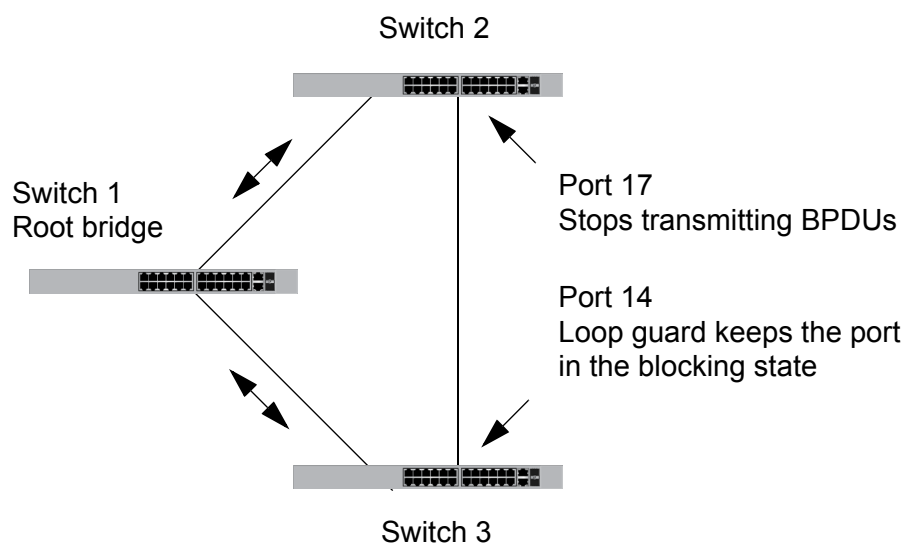
Figure 115. Loop Guard Example 3

The previous example illustrates how loop guard works to maintain a loop-free topology by keeping alternate ports in the blocking state when they stop receiving BPDUs. Loop guard can also work on root and designated ports that are in the forwarding state. This is illustrated in the next two examples.

In the first example, the root bridge stops transmitting BPDUs. If switch 3 is not using loop guard, it continues to forward traffic on port 4. But since no BPDUs are received on the port, it assumes that the device connected to the port is not an RSTP device. Since switch 2 becomes the new root bridge, port 14 on switch 3 transitions to the forwarding state from the blocking state to become the new root port for the switch. The result is a network loop.

Switch 2
New root bridge

Switch 1
Old root bridge
Stops transmitting BPDUs

Port 14
Transitions from the blocking state to the forwarding state

Port 4
Remains in the forwarding state
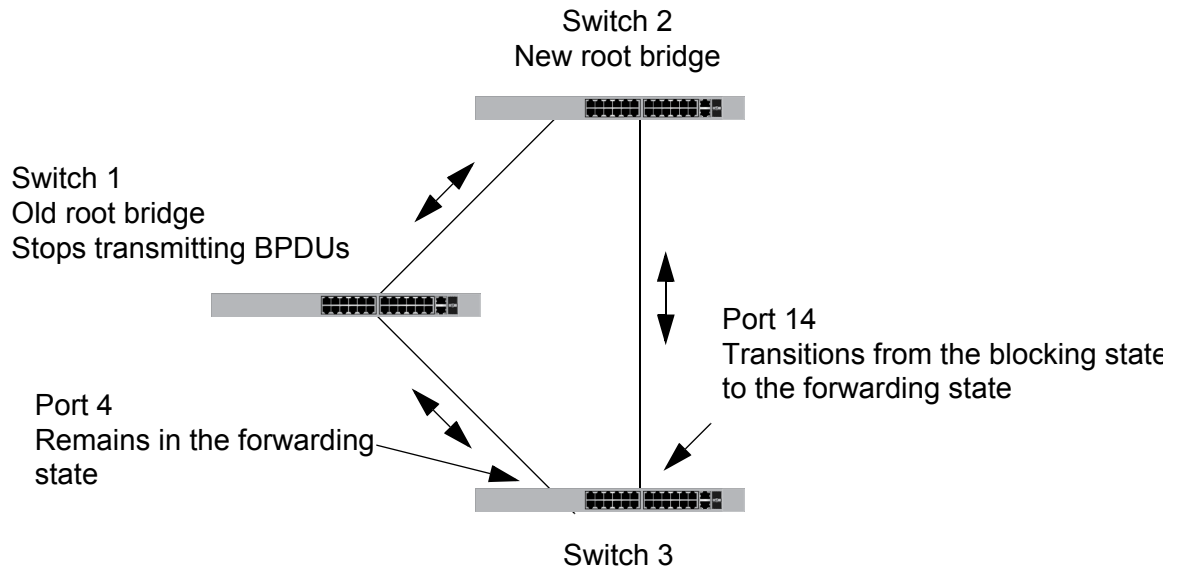
Switch 3

Figure 116. Loop Guard Example 4

But if loop guard is active on port 4 on switch 3, the port is placed in the blocking state since the reception of BPDUs is interrupted. This blocks the loop. The port remains in the blocking state until it again receives BPDUs or the switch is reset.

607

Switch 2
New root bridge

Switch 1
Old root bridge
RSTP stops operating

Port 14
Transitions from the blocking state
to the forwarding state

Port 4
Loop guard changes the
port to the blocking state
from the forwarding state

Switch 3
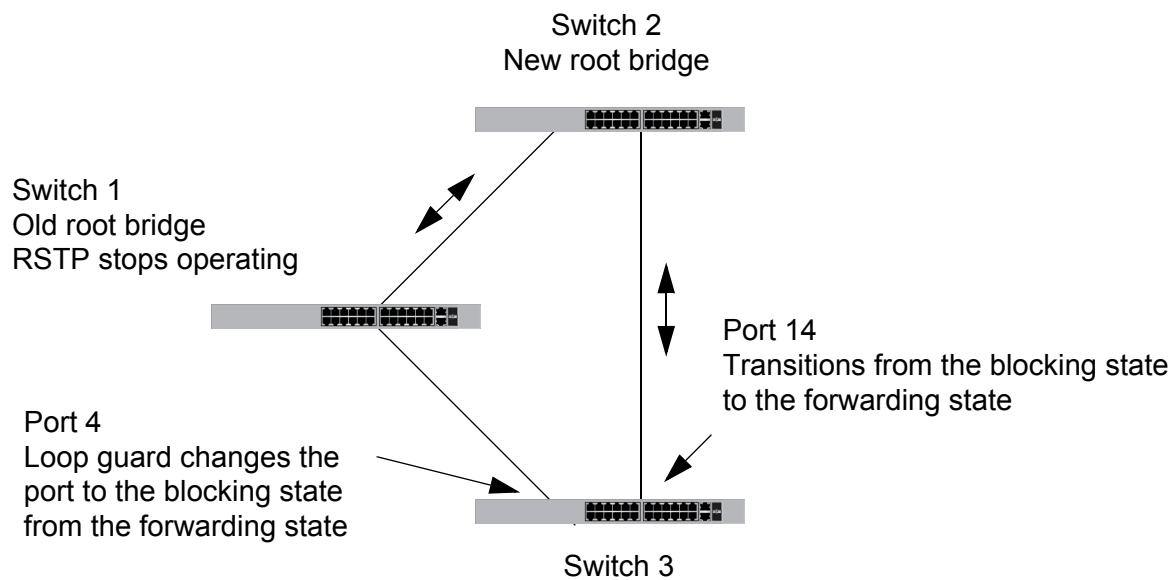
Figure 117. Loop Guard Example 5

STP and RSTP Root Guard

The Root Guard feature enforces the root bridge placement in a network. It ensures the port that you have configured with the Root Guard feature is a designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected.

If the bridge receives a superior BPDU on a root-designated port, the Root Guard feature changes the state of the port to a "root inconsistent" STP state. This state varies depending on the spanning tree designation. For STP, this is a listening state. For RSTP (and MSTP), this is a discarding state. For more information about this command, see "SPANNING-TREE GUARD ROOT" on page 659 in the RSTP Commands chapter.

Note
This feature is also supported in MSTP. See "MSTP Root Guard" on page 689 for more information.

Chapter 41
Spanning Tree Protocol (STP) Procedures

This chapter provides the following procedures:

Designating STP as the Active Spanning Tree Protocol

Before you can configure the STP parameters or enable the protocol on the switch, you have to designate STP as the active spanning tree protocol. The switch supports other spanning tree protocols in addition to STP, but only one of them can be active at a time on the device.

To designate STP as the active spanning tree protocol on the switch, use the SPANNING-TREE MODE STP command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode stp
```

After you enter the command, you can configure the STP parameters and enable the protocol so that the switch begins to use the protocol.

Enabling the Spanning Tree Protocol

To enable STP on the switch, use the SPANNING-TREE STP ENABLE command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

The switch immediately begins to send BPDUs from its ports to participate in the spanning tree domain.

Setting the Switch Parameters

This table lists the STP functions that are controlled at the switch level. These commands are located in the Global Configuration mode and apply to the entire switch.

Table 60. STP Switch Parameter Commands

To	Use This Command	Range
Specify how long the ports remain in the listening and learning states before entering the forwarding state.	SPANNING-TREE FORWARD-TIME *forwardtime*	4 to 30 seconds
Configure how frequently the switch sends spanning tree configuration information when it is functioning as the root bridge or trying to become the root bridge.	SPANNING-TREE HELLO-TIME *hellotime*	1 to 10 seconds
Configure how long the switch stores bridge protocol data units (BPDUs) before deleting them.	SPANNING-TREE MAX-AGE *maxage*	6 to 40 seconds
Assign the switch a priority number, which is used to determine the root bridge in the spanning tree domain.	SPANNING-TREE PRIORITY *priority*	0 to 61,440, in increments of 4,096

Unless you are familiar with their functions, you should not change the forward time, hello time, and max-age parameters from their default values on the switch. These parameters have to be set in accordance with the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age => 2 x (hello time + 1.0 second)

This example changes the forward time to 24 seconds, the hello time to 5 seconds and the max-age to 20:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forward-time 24
awplus(config)# spanning-tree hello-time 5
awplus(config)# spanning-tree max-age 20
```

If you want the switch to be the root bridge of the spanning tree domain, assign it a low priority number with the SPANNING-TREE PRIORITY command. The bridge priority has a range 0 to 61,440 in increments of 4.096. The default value is 32,768.

This example of the command sets the switch's priority value to 8,192:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree priority 8192
```

Setting the Port Parameters

This table lists the STP functions that are controlled at the port level. You set these parameters in the Port Interface mode of the individual ports.

Table 61. STP Port Parameter Commands

To	Use This Command	Range
Specify the cost of a port to the root bridge.	SPANNING-TREE PATH-COST *path-cost*	1 to 200000000
Assign a priority value, which is used as a tie breaker when two or more ports have equal costs to the root bridge.	SPANNING-TREE PRIORITY *priority*	0 to 240 in increments of 16

This example of the SPANNING-TREE PATH-COST command assigns a path cost of 40 to ports 4 and 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.18
awplus(config-if)# spanning-tree path-cost 40
```

This example of the SPANNING-TREE PRIORITY command assigns a priority value of 32:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# spanning-tree priority 32
```

Disabling the Spanning Tree Protocol

To disable STP on the switch, use the NO SPANNING-TREE STP ENABLE command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
```

Note
Before disabling the spanning tree protocol on the switch, display the STP states of the ports and disconnect the network cables from any ports that are in the discarding state. Ports that are in the discarding state begin to forward traffic again when STP is disabled. Leaving the cables connected may result in broadcast storms from network loops. To view the states of the ports, refer to "Displaying STP Settings" on page 618.

Displaying STP Settings

To view the STP settings on the switch, use the SHOW SPANNING-TREE in the Privileged Exec mode. The command has this format:

show spanning-tree [interface *port*]

Use the INTERFACE parameter to view the settings of the specified ports. Otherwise, omit the parameter to view all the ports. Here is an example of the information the command displays:

```
% Default: Spanning Tree up - Enabled
% Default: Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20- Root port 0
% Default: Root Id 8000:00153355ede1
% Default: Bridge Id 8000:00153355ede1
% Default: portfast bpdu-guard disabled
% Default: portfast bpdu-filter disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port Id 8001 - Role Disabled - State Disabled
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 2000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8001 - Priority 128  -
%   port1.0.1: Root 8000:000000000000
%   port1.0.1: Designated Bridge 8000:000000000000
%   port1.0.1: Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Version Spanning Tree Protocol
%   port1.0.1: Current portfast off
%   port1.0.1: Current loop-guard off
%   port1.0.1: Current portfast bpdu-guard off
%   port1.0.1: Current portfast bpdu-filter off
%   port1.0.1: Current root-guard off
%   port1.0.1: Configured Link Type auto
```

Figure 118. SHOW SPANNING-TREE Command for STP

Chapter 42
STP Commands

The STP commands are summarized in Table 62 and described in detail within the chapter.

Table 62. Spanning Tree Protocol Commands

Command	Mode	Description
"NO SPANNING-TREE STP ENABLE" on page 621	Global Configuration	Disables STP on the switch.
"SHOW SPANNING-TREE" on page 622	User Exec and Privileged Exec	Displays the STP settings.
"SPANNING-TREE FORWARD-TIME" on page 624	Global Configuration	Sets the forward time, which specifies how long the ports remain in the listening and learning states before they transition to the forwarding state.
"SPANNING-TREE GUARD ROOT" on page 625	Port Interface	Enables the Root Guard feature on a port.
"SPANNING-TREE HELLO-TIME" on page 626	Global Configuration	Sets the hello time, which defines how frequently the switch sends spanning tree configuration information when it is the root bridge or is trying to become the root bridge.
"SPANNING-TREE MAX-AGE" on page 627	Global Configuration	Sets the maximum age parameter, which defines how long bridge protocol data units (BPDUs) are stored by the switch before they are deleted.
"SPANNING-TREE MODE STP" on page 628	Global Configuration	Designates STP as the active spanning tree protocol on the switch.
"SPANNING-TREE PATH-COST" on page 629	Port Interface	Specifies the cost of a port to the root bridge.
"SPANNING-TREE PORTFAST" on page 630	Port Interface	Designates edge ports on the specified port.

Table 62. Spanning Tree Protocol Commands (Continued)

Command	Mode	Description
"SPANNING-TREE PORTFAST BPDU-GUARD" on page 631	Port Interface	Enables the BPDU guard feature on a port so that the switch monitors edge ports and disables them if they receive BPDUs.
"SPANNING-TREE PRIORITY (Bridge Priority)" on page 632	Global Configuration	Assigns the switch a priority number.
"SPANNING-TREE Priority (Port Priority)" on page 633	Port Interface	Assigns a priority value to a port.
"SPANNING-TREE STP ENABLE" on page 634	Global Configuration	Enables STP on the switch.

NO SPANNING-TREE STP ENABLE

Syntax

```
no spanning-tree stp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable STP on the switch. To view the current status of STP, refer to "SHOW SPANNING-TREE" on page 622. The default setting is disabled.

Note

Before disabling the spanning tree protocol on the switch, display the STP states of the ports and disconnect the network cables from any ports that are in the discarding state. Ports that are in the discarding state begin to forward traffic again when STP is disabled. Leaving the cables connected may result in broadcast storms from network loops. To view the states of the ports, refer to "SHOW SPANNING-TREE" on page 622.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158 or "SHOW SPANNING-TREE" on page 622

Example

This example disables STP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
```

SHOW SPANNING-TREE

Syntax

```
show spanning-tree [interface port]
```

Parameters

port

Specifies a port. You can specify more than one port at a time in the command. The switch displays the STP settings for all the ports if you omit this parameter.

Modes

Privileged Exec mode

Description

Use this command to display the STP settings on the switch. An example of the display is shown in Figure 119.

```
% Default: Spanning Tree up - Enabled
% Default: Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20- Root port 0
% Default: Root Id 8000:00153355ede1
% Default: Bridge Id 8000:00153355ede1
% Default: portfast bpdu-guard disabled
% Default: portfast bpdu-filter disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port Id 8001 - Role Disabled - State Disabled
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 2000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8001 - Priority 128  -
%   port1.0.1: Root 8000:000000000000
%   port1.0.1: Designated Bridge 8000:000000000000
%   port1.0.1: Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Version Spanning Tree Protocol
%   port1.0.1: Current portfast off
%   port1.0.1: Current loop-guard off
%   port1.0.1: Current portfast bpdu-guard off
%   port1.0.1: Current portfast bpdu-filter off
%   port1.0.1: Current root-guard off
%   port1.0.1: Configured Link Type auto
```

Figure 119. SHOW SPANNING-TREE Command for STP

Examples

This command displays the STP settings for all the ports:

```
awplus# show spanning-tree
```

This command displays the STP settings for ports 1 and 4:

```
awplus# show spanning-tree interface port1.0.1,port1.0.4
```

SPANNING-TREE FORWARD-TIME

Syntax

```
spanning-tree forward-time forwardtime
```

Parameters

forwardtime

> Specifies the forward time. The range is 4 to 30 seconds. The default is 15 seconds.

Mode

Global Configuration mode

Description

Use this command to set the forward time parameter on the switch. This parameter specifies how long the ports remain in the listening and learning states before they transition to the forwarding state.

This parameter is active only if the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

The forward time, max-age and hello time parameters should be set according to the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age >= 2 x (hello time + 1.0 second)

Use the no version of this command, NO SPANNING-TREE FORWARD-TIME, to set the command to its default value of 15 seconds.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example sets the forward time on the switch to 25 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forward-time 25
```

SPANNING-TREE GUARD ROOT

Syntax

```
spanning-tree guard root
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable the Root Guard feature on the specified port. The Root Guard feature ensures that the port on which it is enabled is a designated port. If a Root-Guard-enabled port receives a superior BPDU that may cause it to become a root port, then the port traffic is placed in a "root inconsistent" state. For STP, this state is a listening state.

Use the no version of this command, NO SPANNING-TREE GUARD ROOT, to disable the Root Guard feature on the specified port.

To display the current setting for this parameter, refer to "SHOW SPANNING-TREE" on page 622.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Examples

This example enables the Root Guard feature on port 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# spanning-tree guard root
```

This example disables the Root Guard feature on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no spanning-tree guard root
```

SPANNING-TREE HELLO-TIME

Syntax

```
spanning-tree hello-time hellotime
```

Parameters

hellotime
> Specifies the hello time. The range is 1 to 10 seconds. The default is 2 seconds.

Mode

Global Configuration mode

Description

Use this command to set the hello time parameter on the switch. This parameter controls how frequently the switch sends spanning tree configuration information when it is the root bridge or is trying to become the root bridge.

The forward time, max-age and hello time parameters should be set according to the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age >= 2 x (hello time + 1.0 second)

To view the current setting for this parameter, refer to "SHOW SPANNING-TREE" on page 622.

Use the no version of this command, NO SPANNING-TREE HELLO-TIME, to set the command to its default value of 2 seconds.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example sets the hello time parameter on the switch to 7 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree hello-time 7
```

SPANNING-TREE MAX-AGE

Syntax

```
spanning-tree max-age maxage
```

Parameters

maxage
>   Specifies the max-age parameter. The range is 6 to 40 seconds.
>   The default is 20 seconds.

Mode

Global Configuration mode

Description

Use this command to set the maximum age parameter. This parameter determines how long bridge protocol data units (BPDUs) are stored by the switch before they are deleted.

The forward time, max-age and hello time parameters should be set according to the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age => 2 x (hello time + 1.0 second)

Use the no form of this command, NO SPANNING-TREE MAX-AGE, to set the command to its default value of 20 seconds.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example sets the maximum age parameter to 35 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree max-age 35
```

SPANNING-TREE MODE STP

Syntax

```
spanning-tree mode stp
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to designate STP as the active spanning tree protocol on the switch. You must select STP as the active spanning tree protocol before you can enable it or configure its parameters.

Only one spanning tree protocol can be active on the switch at a time.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example designates STP as the active spanning tree protocol on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode stp
```

SPANNING-TREE PATH-COST

Syntax

```
spanning-tree path-cost path-cost
```

Parameters

path-cost
> Specifies the cost of a port to the root bridge. The range is 1 to 200000000.

Mode

Port Interface mode

Description

Use this command to specify the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200000000.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example assigns port 2 a port cost of 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 15
```

SPANNING-TREE PORTFAST

Syntax

```
spanning-tree portfast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to designate an edge port on the switch. Edge ports are not connected to spanning tree devices or to LANs that have spanning tree devices. As a consequence, edge ports do not receive BPDUs. If an edge port starts to receive BPDUs, it is no longer considered to be an edge port.

This command is used in conjunction with the SPANNING-TREE PORTFAST BPDU-GUARD command.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example configures port 17 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# spanning-tree portfast
```

SPANNING-TREE PORTFAST BPDU-GUARD

Syntax

```
spanning-tree portfast bpdu-guard
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable the BPDU guard feature so that the switch monitors edge ports and disables them if they receive BPDU packets.

To disable an edge port that was disabled by the BPDU guard feature, use the NO SPANNING-TREE PORTFAST BPDU-GUARD command. See "NO SPANNING-TREE PORTFAST BPDU-GUARD" on page 652.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example enables the BPDU guard feature on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# spanning-tree portfast bpdu-guard
```

SPANNING-TREE PRIORITY (Bridge Priority)

Syntax

```
spanning-tree priority priority
```

Parameters

priority
> Specifies a priority number for the switch.

Mode

Global Configuration mode

Description

Use this command to assign the switch a priority number. The device that has the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

The range is 0 to 61,440, in increments of 4,096. The priority values can be set only in increments of 4,096. The default value is 32,768.

Use the no form of this command, NO SPANNING-TREE PRIORITY, to reset the command to its default value of 32,768.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example sets the priority value of the switch to 8,192:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree priority 8192
```

SPANNING-TREE Priority (Port Priority)

Syntax

```
spanning-tree priority priority
```

Parameters

priority
> Specifies the priority value for a port. The range is 0 to 240, in increments of 16.

Mode

Port Interface mode

Description

Use this command to set the priority value of a port. This parameter is used as a tie breaker when two or more ports have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The priority values can be set only in increments of 16. The default is 128.

Use the no form of this command, NO SPANNING-TREE PRIORITY, to reset the command to its default value of 128.

Confirmation Command

"SHOW SPANNING-TREE" on page 622

Example

This example assigns ports 16 and 17 a port priority value of 192:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16,port1.0.17
awplus(config-if)# spanning-tree priority 192
```

SPANNING-TREE STP ENABLE

Syntax

```
spanning-tree stp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable STP on the switch. You must designate STP as the active spanning tree protocol on the switch before you can enable it or configure its parameters. For instructions, refer to "SPANNING-TREE MODE STP" on page 628.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158 or "SHOW SPANNING-TREE" on page 622

Example

This example enables STP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

Chapter 43

Rapid Spanning Tree Protocol (RSTP) Procedures

This chapter provides the following procedures:

❒ "Designating RSTP as the Active Spanning Tree Protocol" on page 636

❒ "Enabling the Rapid Spanning Tree Protocol" on page 637

❒ "Configuring the Switch Parameters" on page 638

❒ "Configuring the Port Parameters" on page 641

❒ "Disabling the Rapid Spanning Tree Protocol" on page 645

❒ "Displaying RSTP Settings" on page 646

Designating RSTP as the Active Spanning Tree Protocol

The first step to using RSTP on the switch is to designate it as the active spanning tree protocol. This is accomplished with the SPANNING-TREE MODE RSTP command in the Global Configuration mode. Afterwards, you can configure its settings and enable the protocol. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode rstp
```

Because RSTP is the default active spanning tree protocol on the switch, you only need to use this command if you activated STP and now want to change the switch back to RSTP.

Enabling the Rapid Spanning Tree Protocol

To enable RSTP on the switch, use the SPANNING-TREE RSTP ENABLE command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

After you enter the command, the switch immediately begins to participate in the spanning tree domain. It sends BPDUs from its ports and disables ports if it determines, along with the other STP and RSTP devices, that there are loops in the network topology.

Configuring the Switch Parameters

This table lists the RSTP parameters that are set in the Global Configuration mode and apply to all the ports on the switch.

Table 63. RSTP Switch Parameters

To	Use This Command	Range
Specify how long the ports remain in the listening and learning states before they transition to the forwarding state.	SPANNING-TREE FORWARD-TIME *forwardtime*	4 to 30 seconds
Configure how frequently the switch sends spanning tree configuration information if it is the root bridge or is trying to become the root bridge.	SPANNING-TREE HELLO-TIME *hellotime*	1 to 10 seconds
Configure how long the switch stores bridge protocol data units (BPDUs) before deleting them.	SPANNING-TREE MAX-AGE *maxage*	6 to 40 seconds
Assign the switch a priority number, which is used to determine the root bridge in the spanning tree domain.	SPANNING-TREE PRIORITY *priority*	0 to 61,440, in increments of 4,096
Enable BPDU guard so that the switch disables edge ports if they receive BPDU packets.	SPANNING-TREE PORTFAST BPDU-GUARD	-
Disable BPDU guard on the switch.	NO SPANNING-TREE PORTFAST BPDU-GUARD	-

Setting the Forward Time, Hello Time, and Max Age

You should not change the forward time, hello time, and max-age parameters from their default values unless you are familiar with their functions. These parameters have to be set in accordance with the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age >= 2 x (hello time + 1.0 second)

This example reduces the max-age parameter to discard BPDUs after 10 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree max-age 10
```

This example increases the forward time to 25 seconds and the hello time to 8 seconds. The forward time controls the amount of time the ports remain in the listening and learning states, and the hello time controls how frequently the switch sends spanning tree configuration information:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forward-time 25
awplus(config)# spanning-tree hello-time 8
```

For reference information, refer to "SPANNING-TREE FORWARD-TIME" on page 658, "SPANNING-TREE HELLO-TIME" on page 660 and "SPANNING-TREE MAX-AGE" on page 663.

Setting the Bridge Priority

The bridges of a spanning tree domain use their priority values to determine the root bridge. The lower the value, the higher the priority. The bridge with the highest priority becomes the root bridge. The range of the parameter is 0 to 61,440, in increments of 4,096. The priority values can be set only in increments of 4,096.

This example assigns the switch the low priority number 4,096 to increase the likelihood of it becoming the root bridge of the spanning tree domain:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree priority 4096
```

For reference information, refer to "SPANNING-TREE PRIORITY (Bridge Priority)" on page 668.

Enabling or Disabling BPDU Guard

The BPDU guard feature disables edge ports if they receive BPDU packets. For background information, refer to "RSTP and MSTP BPDU Guard" on page 602. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

After you enter the command, the switch disables any edge ports that receive BPDU packets.

Note
To enable an edge port that was disabled by the BPDU guard feature, use the NO SHUTDOWN command. For instructions, refer to "NO SHUTDOWN" on page 211. If a port is still receiving BPDUs, the switch will disable it again unless you disconnect the network cable.

To disable the BPDU guard feature on the switch, use the NO SPANNING-TREE BPDU-GUARD command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree portfast bpdu-guard
```

Configuring the Port Parameters

This table lists the RSTP port parameters. These parameters are set on the individual ports in the Port Interface mode.

Table 64. RSTP Port Parameters

To	Use This Command	Range
Specify port costs.	SPANNING-TREE PATH-COST *path-cost*	1 to 200000000
Assign a priority value to be used as a tie breaker when two or more paths have equal costs to the root bridge.	SPANNING-TREE PRIORITY *priority*	0 to 240 in increments of 16
Designate edge ports.	SPANNING-TREE PORTFAST	-
Remove the edge port designation from ports.	NO SPANNING-TREE	-
Designate ports as point-to-point or shared links.	SPANNING-TREE LINK-TYPE POINT-TO-POINT|SHARED	-
Enable the loop-guard feature.	SPANNING-TREE LOOP-GUARD	-
Disable the loop-guard feature.	NO SPANNING-TREE LOOP-GUARD	-
Activate the BPDU guard feature.	SPANNING-TREE PORTFAST BPDU-GUARD	-
Activate the BPDU guard timer.	SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE	-
Specify the time interval.	SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL	10 to 1000000 seconds
Deactivate the BPDU guard timer.	NO SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE	-

Configuring Port Costs

The command to change the costs of the ports is the SPANNING-TREE PATH-COST command. The lower the port cost, the greater the likelihood a port will be selected as part of the active path to the root bridge if there is a physical loop in the topology.

This example assigns a port cost of 12 to port 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 12
```

641

Configuring Port Priorities

If RSTP discovers a loop in the topology, but the two paths that constitute the loop have the same path cost, the spanning tree protocol uses port priorities to determine which path to make active and which to place in the blocking state. The lower the priority value, the higher the priority and the greater the likelihood of a port being the active, designated port in the event of duplicate paths.

The range is 0 to 240, in increments of 16. The priority values can be set only in increments of 16. The default value is 128.

This example assigns ports 20 and 21 a port priority value of 192:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20,port1.0.21
awplus(config-if)# spanning-tree priority 192
```

Designating Point-to-point and Shared Ports

This example designates ports 11 to 23 as point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.23
awplus(config-if)# spanning-tree link-type point-to-point
```

This example designates ports 26 and 27 as shared ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.26,port1.0.27
awplus(config-if)# spanning-tree link-type shared
```

Designating Edge Ports

If a port on the switch is not connected to a device or a network that is running the spanning tree protocol, you can designate it as an edge port to reduce the time of the spanning tree convergence process. Edge ports are not taken into account in the convergence process. If a port that has been designated as an edge port begins to receive RSTP BPDUs, the switch automatically considers it as a non-edge port.

To designate ports as edge ports, use the SPANNING-TREE PORTFAST command. This example configures port 16 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# spanning-tree portfast
```

642

This example uses the NO SPANNING-TREE command to remove port 21 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# no spanning-tree portfast
```

Enabling or Disabling RSTP Loop-guard

The RSTP loop guard feature disables ports if they stop receiving spanning tree BPDUs from their link partners when there is no change to the link state. For background information, refer to "STP, RSTP, MSTP Loop Guard" on page 604. In this example, the feature is activated on ports 20 and 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20,port1.0.21
awplus(config-if)# spanning-tree loop-guard
```

A port disabled by this feature remains disabled until it starts to receive BPDU packets again or the switch is reset.

To disable the loop-guard feature, use the NO SPANNING-TREE LOOP-GUARD command. This example disables the feature on port 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no spanning-tree loop-guard
```

Note
Ports disabled by the loop-guard feature do not forward traffic again when you disable the feature. They only forward traffic if they receive BPDUs again or you reset the switch.

Enabling or Disabling BPDU Guard

The BPDU guard feature disables edge ports that receive BPDU packets. For background information, refer to "RSTP and MSTP BPDU Guard" on page 602. This example activates the feature on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

Edge ports that are disabled by the feature remain disabled until you manually enable them again with the NO SHUTDOWN command. As an alternative, you can activate the BPDU guard timer so that the switch automatically reactivates disabled ports after the specified period of time. This example activates the timer and sets it to 1000 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout enable
awplus(config)# spanning-tree errdisable-timeout interval
1000
```

To disable BPDU guard on the switch, use the NO SPANNING-TREE PORTFAST BPDU-GUARD command, shown in this example:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree portfast bpdu guard
```

644

Disabling the Rapid Spanning Tree Protocol

To disable RSTP on the switch, use the NO SPANNING-TREE RSTP ENABLE command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
```

To view the current status of RSTP, refer to "Displaying RSTP Settings" on page 646.

Note

Before disabling the spanning tree protocol on the switch, display the RSTP states of the ports and disconnect the network cables from any ports that are in the discarding state. Ports that are in the discarding state begin to forward traffic again when RSTP is disabled. Leaving the cables connected may result in broadcast storms from network loops. To view the states of the ports, refer to "Displaying RSTP Settings" on page 646.

Displaying RSTP Settings

To view the RSTP settings on the switch, use the SHOW SPANNING-TREE in the Privileged Exec mode. The command has this format:

show spanning-tree [interface *port*]

Use the INTERFACE parameter to view the settings of the specified ports. Otherwise, omit the parameter to view all the ports. Here is an example of the information the command displays:

```
% Default: Bridge up - Spanning Tree Disabled
% Default: Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 8000:eccd6d4d5bf9
% Default: Bridge Id 8000:eccd6d4d5bf9
% Default: portfast bpdu-guard disabled
% Default: portfast bpdu-filter disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port Id 8101 - Role Disabled - State Forwarding
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 2000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8101 - Priority 128  -
%   port1.0.1: Root 8000:000000000000
%   port1.0.1: Designated Bridge 8000:000000000000
%   port1.0.1: Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Version Rapid Spanning Tree Protocol
%   port1.0.1: Current portfast off
%   port1.0.1: Current loop-guard off
%   port1.0.1: Current portfast bpdu-guard off
%   port1.0.1: Current portfast bpdu-filter off
%   port1.0.1: Current root-guard off
%   port1.0.1: Configured Link Type auto
```

Figure 120. SHOW SPANNING-TREE Command for RSTP

Chapter 44
RSTP Commands

The RSTP commands are summarized in Table 65 and described in detail within the chapter.

Table 65. Rapid Spanning Tree Protocol Commands

Command	Mode	Description
"NO SPANNING-TREE PORTFAST" on page 649	Port Interface	Removes ports as edge ports on the switch.
"NO SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 650	Global Configuration	Deactivates the RSTP BPDU guard timer.
"NO SPANNING-TREE LOOP-GUARD" on page 651	Port Interface	Disables the BPDU loop-guard feature on the ports.
"NO SPANNING-TREE PORTFAST BPDU-GUARD" on page 652	Port Interface	Disables the BPDU guard feature on a port.
"NO SPANNING-TREE RSTP ENABLE" on page 653	Global Configuration	Disables RSTP on the switch.
"SHOW SPANNING-TREE" on page 654	User Exec and Privileged Exec	Displays the RSTP settings on the switch.
"SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 656	Global Configuration	Activates the RSTP BPDU guard timer.
"SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL" on page 657	Global Configuration	Specifies the duration the RSTP BPDU guard timer.
"SPANNING-TREE FORWARD-TIME" on page 658	Global Configuration	Sets the forward time, which specifies how long ports remain in the listening and learning states before they transition to the forwarding state.
"SPANNING-TREE GUARD ROOT" on page 659	Port Interface	Enables the Root Guard feature on a port.
"SPANNING-TREE HELLO-TIME" on page 660	Global Configuration	Sets the hello time, which defines how frequently the switch sends spanning tree configuration information when it is the root bridge or is trying to become the root bridge.

Table 65. Rapid Spanning Tree Protocol Commands (Continued)

Command	Mode	Description
"SPANNING-TREE LINK-TYPE" on page 661	Port Interface	Designates point-to-point ports and shared ports.
"SPANNING-TREE LOOP-GUARD" on page 662	Port Interface	Enables the BPDU loop-guard feature on the ports.
"SPANNING-TREE MAX-AGE" on page 663	Global Configuration	Sets the maximum age parameter, which defines how long bridge protocol data units (BPDUs) are stored by the switch before they are deleted.
"SPANNING-TREE MODE RSTP" on page 664	Global Configuration	Designates RSTP as the active spanning tree protocol on the switch.
"SPANNING-TREE PATH-COST" on page 665	Port Interface	Specifies the costs of the ports to the root bridge.
"SPANNING-TREE PORTFAST" on page 666	Port Interface	Designates the ports as edge ports.
"SPANNING-TREE PORTFAST BPDU-GUARD" on page 667	Port Interface	Enables the BPDU guard feature on a port.
"SPANNING-TREE PRIORITY (Bridge Priority)" on page 668	Global Configuration	Assigns the switch a priority number.
"SPANNING-TREE PRIORITY (Port Priority)" on page 669	Port Interface	Assigns priority values to the ports.
"SPANNING-TREE RSTP ENABLE" on page 670	Global Configuration	Enables RSTP on the switch.

NO SPANNING-TREE PORTFAST

Syntax

```
no spanning-tree portfast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove ports as edge ports on the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example removes port 21 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# no spanning-tree portfast
```

NO SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE

Syntax

```
no spanning-tree errdisable-timeout enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to deactivate the timer for the RSTP BPDU guard feature. When the timer is deactivated, ports that the feature disables because they receive BPDU packets remain disabled until you manually activate them again with the NO SHUTDOWN command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example deactivates the time for the RSTP BPDU guard feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree errdisable-timeout enable
```

NO SPANNING-TREE LOOP-GUARD

Syntax

```
no spanning-tree loop-guard
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the BPDU loop-guard feature on the ports. The default setting is disabled.

Note
Ports that are disabled by the loop-guard feature do not forward traffic again when you disable the feature. They only forward traffic if they start to receive BPDUs again or you reset the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example disables the BPDU loop-guard feature on port 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no spanning-tree loop-guard
```

NO SPANNING-TREE PORTFAST BPDU-GUARD

Syntax

```
no spanning-tree portfast bpdu-guard
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the BPDU guard feature on a port.

Note
Edge ports disabled by the BPDU guard feature remain disabled
until you enable them with the management software. For
instructions, refer to "NO SHUTDOWN" on page 211.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example disables the guard feature on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no spanning-tree portfast bpdu-guard
```

NO SPANNING-TREE RSTP ENABLE

Syntax

```
no spanning-tree rstp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable RSTP on the switch.

Note

Before disabling the spanning tree protocol on the switch, display the RSTP states of the ports and disconnect the network cables from any ports that are in the discarding state. Ports that are in the discarding state begin to forward traffic again when RSTP is disabled. Leaving the cables connected may result in broadcast storms from network loops. To view the states of the ports, refer to "SHOW SPANNING-TREE" on page 654.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example disables RSTP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
```

SHOW SPANNING-TREE

Syntax

show spanning-tree

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the RSTP settings on the switch. An example of the display is shown in Figure 121.

```
% Default: Bridge up - Spanning Tree Disabled
% Default: Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 8000:eccd6d4d5bf9
% Default: Bridge Id 8000:eccd6d4d5bf9
% Default: portfast bpdu-guard disabled
% Default: portfast bpdu-filter disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port Id 8101 - Role Disabled - State Forwarding
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 2000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8101 - Priority 128  -
%   port1.0.1: Root 8000:000000000000
%   port1.0.1: Designated Bridge 8000:000000000000
%   port1.0.1: Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Version Rapid Spanning Tree Protocol
%   port1.0.1: Current portfast off
%   port1.0.1: Current loop-guard off
%   port1.0.1: Current portfast bpdu-guard off
%   port1.0.1: Current portfast bpdu-filter off
%   port1.0.1: Current root-guard off
%   port1.0.1: Configured Link Type auto
```

Figure 121. SHOW SPANNING-TREE Command for RSTP

Example

This example displays the RSTP settings on the switch:

```
awplus# show spanning-tree
```

SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE

Syntax

```
spanning-tree errdisable-timeout enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the timer for the RSTP BPDU guard feature. The BPDU guard feature prevents unnecessary RSTP domain convergences by disabling edge ports if they receive BPDUs. When the timer is activated, the switch will automatically reactivate disabled ports. The time interval that ports remain disabled is set with "SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL" on page 657.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example activates the timer for the RSTP BPDU guard feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout enable
```

SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL

Syntax

```
spanning-tree errdisable-timeout interval interval
```

Parameters

interval

Specifies the number of seconds that ports remain disabled by the RSTP BPDU guard feature. The range is 10 to 1000000 seconds. The default is 300 seconds.

Mode

Global Configuration mode

Description

Use this command to specify the number of seconds that must elapse before the switch automatically enables ports that are disabled by the RSTP BPDU guard feature. To activate the timer, refer to "SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 656.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the time interval to 200 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout interval
200
```

SPANNING-TREE FORWARD-TIME

Syntax

```
spanning-tree forward-time forwardtime
```

Parameters

forwardtime
> Specifies the forward time. The range is 4 to 30 seconds. The default is 15 seconds.

Mode

Global Configuration mode

Description

Use this command to set the forward time parameter to control how fast the ports change their spanning tree states when moving towards the forwarding state. For RSTP, this parameter specifies the maximum time taken by the ports to transition from the discarding state to the learning state and from the learning state to the forwarding state.

This parameter is active only if the switch is acting as the root bridge. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

The forward time, max-age and hello time parameters should be set according to the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age >= 2 x (hello time + 1.0 second)

Use the no version of this command, NO SPANNING-TREE FORWARD-TIME, to set the command to its default value of 15 seconds.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example sets the forward time for the switch to 5 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forward-time 5
```

SPANNING-TREE GUARD ROOT

Syntax

```
spanning-tree guard root
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable the Root Guard feature on the specified port. The Root Guard feature ensures that the port on which it is enabled is a designated port. If a Root-Guard-enabled port receives a superior BPDU that may cause it to become a root port, then the port traffic is placed in a "root inconsistent" state. For RSTP, this state is a discarding state.

Use the no version of this command, NO SPANNING-TREE GUARD ROOT, to disable the Root Guard feature on the specified port.

To view the current setting for this parameter, refer to "SHOW SPANNING-TREE" on page 654.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Examples

This example enables the Root Guard feature on port 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# spanning-tree guard root
```

This example disables the Root Guard feature on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no spanning-tree guard root
```

SPANNING-TREE HELLO-TIME

Syntax

```
spanning-tree hello-time hellotime
```

Parameters

hellotime
> Specifies the hello time. The range is 1 to 10 seconds. The default is 2 seconds.

Mode

Global Configuration mode

Description

Use this command to set the hello time parameter on the switch. This parameter controls how frequently the switch sends spanning tree configuration information when it is the root bridge or is trying to become the root bridge.

The forward time, max-age and hello time parameters should be set according to the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age >= 2 x (hello time + 1.0 second)

Use the no version of this command, NO SPANNING-TREE HELLO-TIME, to set the command to its default value of 2 seconds.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example sets the hello time parameter on the switch to 4 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree hello-time 4
```

SPANNING-TREE LINK-TYPE

Syntax

```
spanning-tree link-type point-to-point|shared
```

Parameters

point-to-point
> Allows for rapid transition of a port to the forwarding state during the convergence process of the spanning tree domain.

shared
> Disables rapid transition of a port. You may want to set link type to shared if a port is connected to a hub with multiple switches connected to it.

Mode

Port Interface mode

Description

Use this command to designate point-to-point ports and shared ports.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example designates ports 11 to 23 as point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.23
awplus(config-if)# spanning-tree link-type point-to-point
```

This example designates the links on ports 26 and 27 as shared links:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.26,port1.0.27
awplus(config-if)# spanning-tree link-type shared
```

SPANNING-TREE LOOP-GUARD

Syntax

```
spanning-tree loop-guard
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable the BPDU loop-guard feature on the ports. If a port that has this feature activated stops receiving BPDU packets, the switch automatically disables it. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example activates the BPDU loop-guard feature on ports 5 and 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.11
awplus(config-if)# spanning-tree loop-guard
```

SPANNING-TREE MAX-AGE

Syntax

spanning-tree max-age *maxage*

Parameters

maxage
> Specifies the maximum age parameter. The range is 6 to 40 seconds. The default is 20 seconds.

Mode

Global Configuration mode

Description

Use this command to set the maximum age parameter on the switch. This parameter determines how long the switch retains bridge protocol data units (BPDUs) before it deletes them.

The forward time, maximum age and hello time parameters should be set according to the following formulas, as specified in IEEE Standard 802.1d:

max-age <= 2 x (forward time - 1.0 second)
max-age >= 2 x (hello time + 1.0 second)

Use the no form of this command, NO SPANNING-TREE MAX-AGE, to set the command to its default value of 20 seconds.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example sets the maximum age parameter to 10 seconds:

awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree max-age 10

SPANNING-TREE MODE RSTP

Syntax

```
spanning-tree mode rstp
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to designate RSTP as the active spanning tree protocol on the switch. After activating the protocol, you can enable or disable the spanning tree protocol and set the switch or port parameters. RSTP is active on the switch only after you have designated it as the active spanning tree with this command and enabled it with "SPANNING-TREE RSTP ENABLE" on page 670.

Only one spanning tree protocol— STP or RSTP— can be active on the switch at a time.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example designates RSTP as the active spanning tree protocol on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode rstp
```

SPANNING-TREE PATH-COST

Syntax

```
spanning-tree path-cost path-cost
```

Parameters

path-cost
>   Specifies the cost of a port to the root bridge. The range is 1 to 200000000.

Mode

Port Interface mode

Description

Use this command to specify the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of a path. The range is 1 to 200000000.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example assigns a port cost of 22 to port 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 22
```

SPANNING-TREE PORTFAST

Syntax

```
spanning-tree portfast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to designate edge ports on the switch. Edge ports are not connected to spanning tree devices or to LANs that have spanning tree devices. As a consequence, edge ports do not receive BPDUs. If an edge port starts to receive BPDUs, it is no longer considered an edge port by the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example configures port 17 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# spanning-tree portfast
```

SPANNING-TREE PORTFAST BPDU-GUARD

Syntax

```
spanning-tree portfast bpdu-guard
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable the BPDU guard feature so that the switch monitors edge ports and disables them if they receive BPDU packets.

To disable an edge port that was disabled by the BPDU guard feature, use the NO SPANNING-TREE PORTFAST BPDU-GUARD command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example enables the BPDU guard feature on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# spanning-tree portfast bpdu-guard
```

SPANNING-TREE PRIORITY (Bridge Priority)

Syntax

```
spanning-tree priority priority
```

Parameters

priority
> Specifies a priority number for the switch. The range is 0 to 61440, in increments of 4096.

Mode

Global Configuration mode

Description

Use this command to assign the switch a priority number. The device that has the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

The range is 0 to 61,440, in increments of 4,096. The priority value can be set only in increments of 4,096. The default value is 32,768.

Use the no form of this command, NO SPANNING-TREE PRIORITY, to reset the command to its default value of 32,768.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example sets the priority value of the switch to 8,192:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree priority 8192
```

SPANNING-TREE PRIORITY (Port Priority)

Syntax

```
spanning-tree priority priority
```

Parameters

priority
    Specifies the priority value for a port. The range is 0 to 240, in increments of 16.

Mode

Port Interface mode

Description

Use this command to set the priority value of a port. This parameter is used as a tie breaker when two or more ports have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The priority values can be set only in increments of 16. The default is 128.

Use the no form of this command, NO SPANNING-TREE PRIORITY, to reset the command to its default value of 128.

Confirmation Command

"SHOW SPANNING-TREE" on page 654

Example

This example assigns ports 20 and 21 a port priority value of 192:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20,port1.0.21
awplus(config-if)# spanning-tree priority 192
```

SPANNING-TREE RSTP ENABLE

Syntax

```
spanning-tree rstp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the Rapid Spanning Tree Protocol on the switch. You cannot enable RSTP until you have activated it with "SPANNING-TREE MODE RSTP" on page 664.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158 or "SHOW SPANNING-TREE" on page 654

Example

This example enables RSTP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

Chapter 45

Multiple Spanning Tree Protocol (MSTP)

This chapter provides background information about the Multiple Spanning Tree Protocol (MSTP). It covers the following topics:

Overview

As mentioned in Chapter 40, "STP, RSTP and MSTP Protocols" on page 591, STP and RSTP are referred to as single-instance spanning trees that search for physical loops across all VLANs in a bridged network. When loops are detected, the protocols stop the loops by placing one or more bridge ports in a blocking state.

As explained in "Spanning Tree and VLANs" on page 601, STP and RSTP can result in VLAN fragmentation where VLANs that span multiple bridges are connected together with untagged ports. The untagged ports creating the links can represent a physical loop in the network, which are blocked by spanning tree. This can result in a loss of communication between different parts of the same VLAN.

One way to resolve this, other than by not activating spanning tree on your network, is to link the switches using tagged ports, which can handle traffic from multiple VLANs simultaneously. The drawback to this approach is that the link formed by the tagged ports can create a bottleneck to your Ethernet traffic, resulting in reduced network performance.

Another approach is to use the Multiple Spanning Tree Protocol (MSTP). This spanning tree shares many of the same characteristics as RSTP. It features rapid convergence and has many of the same parameters. But the main difference is that while RSTP, just like STP, supports only a single-instance spanning tree, MSTP supports multiple spanning trees within a network.

The following sections describe some of the terms and concepts relating to MSTP. If you are not familiar with spanning tree or RSTP, review "Overview" on page 592.

> **Note**
> Do not activate MSTP on an AT-9000 Allied Telesis Switch without first familiarizing yourself with the following concepts and guidelines. Unlike STP and RSTP, you cannot activate this spanning tree protocol on a switch without first configuring the protocol parameters.

> **Note**
> The AlliedWare Plus MSTP implementation complies fully with the new IEEE 802.1s standard and should be interoperable with any other vendor's fully compliant 802.1s implementation.

672

Multiple Spanning Tree Instance (MSTI)

The individual spanning trees in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). An MSTI can span any number of AT-9000 Switches. The switch can support up to 15 MSTIs at a time.

To create an MSTI, you first assign it a number, referred to as the MSTI ID. The range is 1 to 15. (The switch is shipped with a default MSTI with an MSTI ID of 0. This default spanning tree instance is discussed later in "Common and Internal Spanning Tree (CIST)" on page 681.)

After you have selected an MSTI ID, you need to define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Following are several examples. Figure 122 illustrates two AT-9000 Switches, each containing the two VLANs Sales and Production. The two parts of each VLAN are connected with a direct link using untagged ports on both switches. If the switches were running STP or RSTP, one of the links would be blocked because the links constitute a physical loop. Which link would be blocked depends on the STP or RSTP bridge settings. In Figure 122, the link between the two parts of the Production VLAN is blocked, resulting in a loss of communications between the two parts of the Production VLAN.
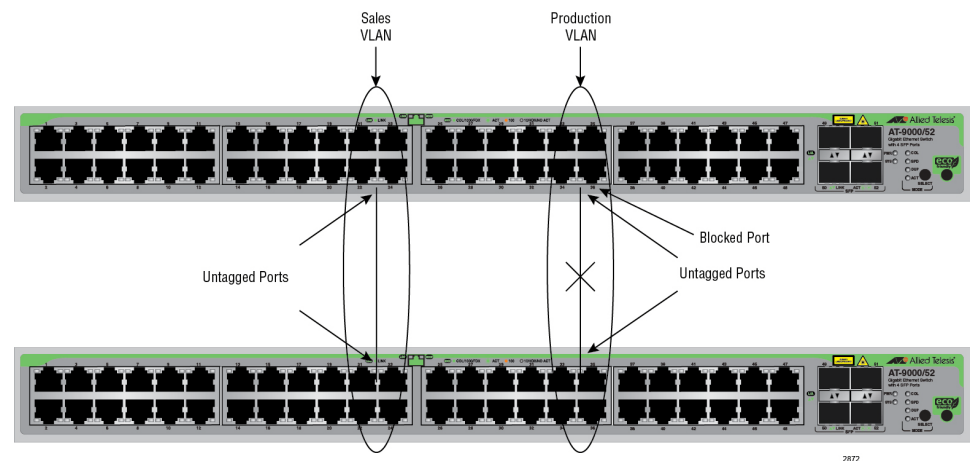
Figure 122. VLAN Fragmentation with STP or RSTP

Figure 123 on page 674 illustrates the same two AT-9000 Switches and the same two virtual LANs. But in this example, the two switches are running MSTP, and the two VLANs have been assigned different spanning tree instances. Now that they reside in different MSTIs, both links remain active, enabling the VLANs to forward traffic over their respective direct link.

673
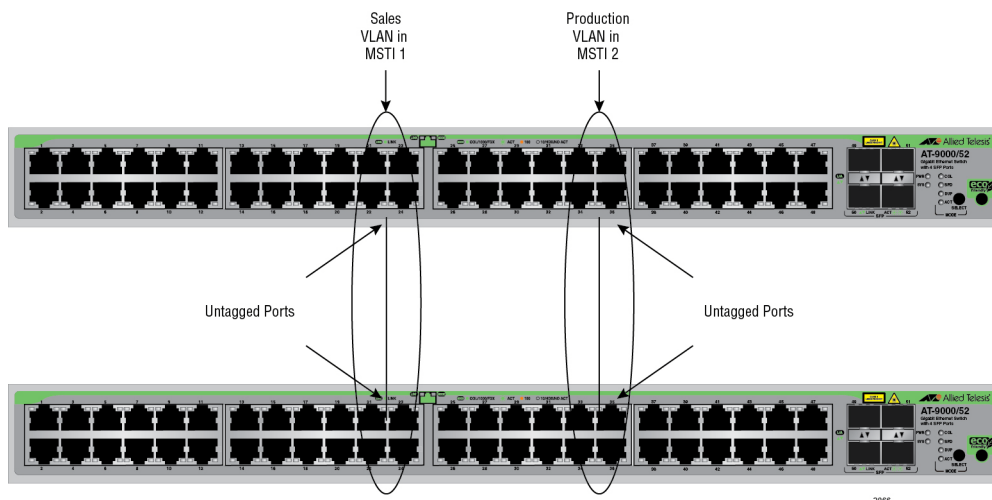
Figure 123. MSTP Example of Two Spanning Tree Instances

An MSTI can contain more than one VLAN. This is illustrated in Figure 124 where there are two AT-9000 Switches with four VLANs. There are two MSTIs, each containing two VLANs. MSTI 1 contains the Sales and Presales VLANs and MSTI 2 contains the Design and Engineering VLANs.
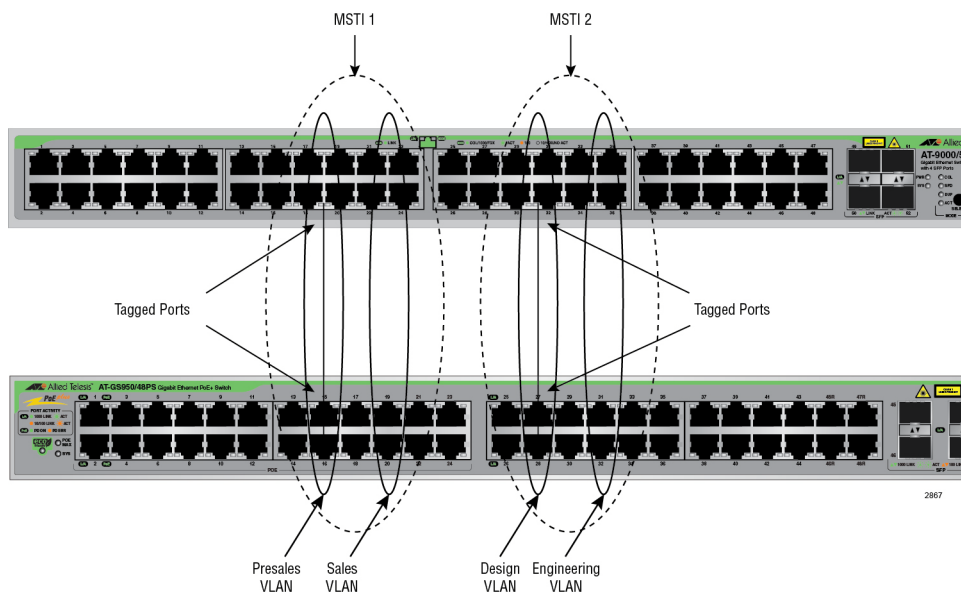
Figure 124. Multiple VLANs in an MSTI

In this example, because an MSTI contains more than one VLAN, the links between the VLAN parts are made with tagged, not untagged, ports so that they can carry traffic from more than one virtual LAN. Referring again to Figure 124, the tagged link in MSTI 1 is carrying traffic for both the Presales and Sales VLANs while the tagged link in MSTI 2 is carrying traffic for the Design and Engineering VLANs.

674

MSTI Guidelines

Following are several guidelines to keep in mind about MSTIs:

❒ The AT-9000 Switch can support up to 15 spanning tree instances, including the Common and Internal Spanning Tree (CIST).

❒ An MSTI can contain any number of VLANs.

❒ A VLAN can belong to only one MSTI at a time.

❒ A switch port can belong to more than one spanning tree instance at a time by being an untagged and tagged member of VLANs belonging to different MSTIs. This is possible because a port can be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance. For further information, refer to "Ports in Multiple MSTIs" on page 677.

❒ A router or Layer 3 network device is required to forward traffic between different VLANs.

VLAN and MSTI Associations

Part of the task to configuring MSTP involves assigning VLANs to spanning tree instances. The mapping of VLANs to MSTIs is called *associations*. A VLAN, either port-based or tagged, can belong to only one instance at a time, but an instance can contain any number of VLANs.

Ports in Multiple MSTIs

A port can be a member of more than one MSTI at a time if it is a tagged member of one or more VLANs assigned to different MSTIs. In this circumstance, a port might be have to operate in different spanning tree states simultaneously, depending on the requirements of the MSTIs. For example, a port that belongs to two different VLANs in two different MSTIs might operate in the forwarding state in one MSTI and the blocking state in the other.

A port's MSTI parameter settings are divided into two groups. The first group is referred to as generic parameters. These are set just once on a port and apply to all the MSTIs where the port is a member. One of these parameters is the external path cost, which sets the operating cost of a port connected to a device outside its region. A port, even if it belongs to multiple MSTIs, can have only one external path cost. Other generic parameters designate the port as an edge port or a point-to-point port.

The second group of port parameters can be set differently for each MSTI where a port is a member. One parameter, the internal path cost, specifies the operating cost of a port when it is connected to a bridge in the same MSTP region. The other parameter in this group sets the port priority, which acts as a tie breaker when two or more ports have equal costs to a regional root bridge.

Multiple Spanning Tree Regions

Another important concept of MSTP is *regions*. An MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. These characteristics are:

- ❐ Configuration name
- ❐ Revision number
- ❐ VLANs
- ❐ VLAN to MSTI ID associations

A *configuration name* is a name assigned to a region to identify it. You must assign each bridge in a region exactly the same name, even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. Examples are Sales Region and Engineering Region.

The *revision number* is an arbitrary number assigned to a region. This number can be used to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is not important that you maintain this number, only that each bridge in a region has the same number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be the same on all bridges of a region.

Finally, the VLANs in the bridges must be associated to the same MSTIs.

If any of the above information is different on two bridges, MSTP does consider the bridges as residing in different regions.

678

Table 66 illustrates the concept of regions. It shows one MSTP region consisting of two AT-9000 Switches. Each switch in the region has the same configuration name and revision level. The switches also have the same five VLANs, and the VLANs are associated with the same MSTIs.

Table 66. MSTP Region

Configuration Name: Marketing Region, Revision Level 1	
Switch 1	**Switch 2**
MSTI ID 1: VLAN: Sales (VID 2) VLAN: Presales (VID 3)	MSTI ID 1: VLAN: Sales (VID 2) VLAN: Presales (VID 3)
MSTI ID 2: VLAN: Accounting (VID 4)	MSTI ID 2: VLAN: Accounting (VID 4)

The AT-9000 Switch determines regional boundaries by examining the MSTP BPDUs received on the ports. A port that receives an MSTP BPDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for any ports connected to bridges running the single-instance spanning tree STP or RSTP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops within the spanning tree instance. An MSTI's root bridge is called a *regional root*. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root for an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the *MSTI priority* value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, MSTI priority is used only to determine the regional root for a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority, from 0 to 61,440 in sixteen increments of 4,096. To set the parameter, you specify the increment that represents the desired MSTI priority value. Table 69 on page 693 lists the increments.

Region Guidelines

Following are several points to remember about regions.

❐ A network can contain any number of regions, and a region can contain any number of AT-9000 Switches.

❐ The AT-9000 Switch can belong to only one region at a time.

❐ A region can contain any number of VLANs.

❐ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.

❐ An MSTI cannot span multiple regions.

❐ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.

❐ The regional root of an MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs that you create yourself. Firstly, you cannot delete this instance, and you cannot change its MSTI ID.

Secondly, when you create a new port-based or tagged VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The Default_VLAN is also associated by default with CIST.

Another critical difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP single-instance spanning trees in the network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and single-instance spanning tree, to form one spanning tree for the entire bridged network.

MSTP uses CIST to form the spanning tree of an entire bridged network because CIST can cross regional boundaries, while an MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and single-instance spanning trees in the bridged network.

The CIST regional root is set with the *CIST Priority* parameter. This parameter, which functions similar to the RSTP bridge priority value, selects the root bridge for the entire bridged network. If the AT-9000 switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all the MSTP regions and STP and RSTP single-instance spanning trees in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on the AT-9000 switch running MSTP receives STP BPDUs, the port sends only STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs because RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered to be a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions and STP and RSTP single-instance spanning trees cannot discern the topology or constitution of an MSTP region. The only bridge they are aware of is the regional root of the CIST instance.

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all the rules and guidelines mentioned in earlier sections, and contains a few new ones:

❒ The AT-9000 Switch can support up to 15 spanning tree instances, including the CIST.

❒ An MSTI can contain any number of VLANs.

❒ A VLAN can belong to only one MSTI at a time.

❒ The range of an MSTI ID is from 1 to 15.

❒ The CIST ID is 0. You cannot change this value.

❒ A switch port can belong to more than one spanning tree instance at a time. This allows you to assign a port as an untagged and tagged member of VLANs that belong to different MSTIs. What makes this possible is a port's ability to be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance.

❒ A router or Layer 3 network device is required to forward traffic between VLANs.

❒ A network can contain any number of regions, and a region can contain any number of AT-9000 Switches.

❒ The AT-9000 Switch can belong to only one region at a time.

❒ A region can contain any number of VLANs.

❒ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.

❒ An MSTI cannot span multiple regions.

❒ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.

❒ The regional root of an MSTI must be in the same region as the MSTI.

❒ The CIST must have a regional root for communicating with other regions and single-instance spanning trees.

❒ MSTP is compatible with STP and RSTP.

❒ A port transmits CIST information even when it is associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained in more detail in "Associating VLANs to MSTIs" on page 685.)

683

Note
The AlliedWare Plus MSTP implementation complies fully with the new IEEE 802.1s standard. Any other vendor's fully compliant 802.1s implementation is interoperable with the AlliedWare Plus implementation.

Associating VLANs to MSTIs

Allied Telesis recommends that you assign all VLANs on a switch to an MSTI. You should not leave a VLAN assigned to just the CIST, including the Default_VLAN. This is to prevent the blocking of a port that should be in the forwarding state. The reason for this guideline is explained below.

An MSTP BPDU contains the instance to which the port transmitting the packet belongs. By default, all ports belong to the CIST instance. So CIST is included in the BPDU. If the port is a member of a VLAN that has been assigned to another MSTI, that information is also included in the BPDU.

This is illustrated in Figure 125. Port 8 in switch A is a member of a VLAN assigned to MSTI ID 7 while port 1 is a member of a VLAN assigned to MSTI ID 10. The BPDUs transmitted by port 8 to switch B would indicate that the port is a member of both CIST and MSTI 7, while the BPDUs from port 1 would indicate the port is a member of the CIST and MSTI 10.
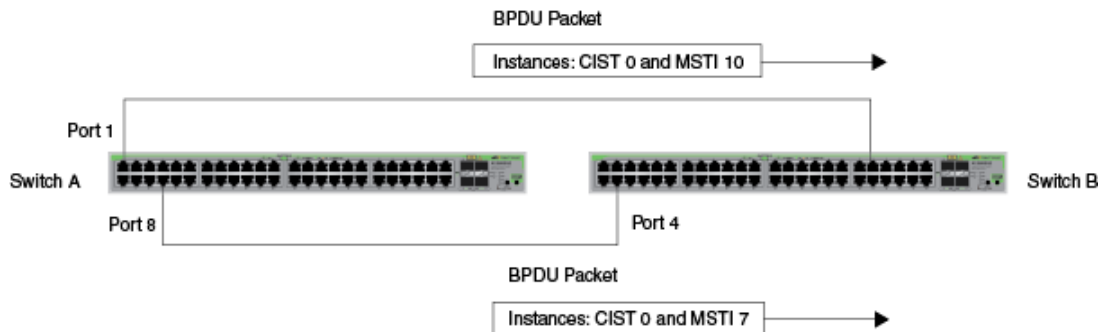
Figure 125. CIST and VLAN Guideline - Example 1

At first glance, it might appear that because both ports belong to CIST, a loop exists between the switches and that MSTP blocks a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When switch B receives a packet from switch A, it uses MSTI, not CIST, to determine whether a loop exists. Because both ports on switch A belong to different MSTIs, switch B determines that no loop exists.

A problem can arise if you assign some VLANs to MSTIs while leaving others just to CIST. The problem is illustrated in Figure 126 on page 686. The network is the same as the previous example. The only difference is that the VLAN containing port 8 on Switch A is not assigned to an MSTI, and belongs only to CIST with its MSTI ID of 0.
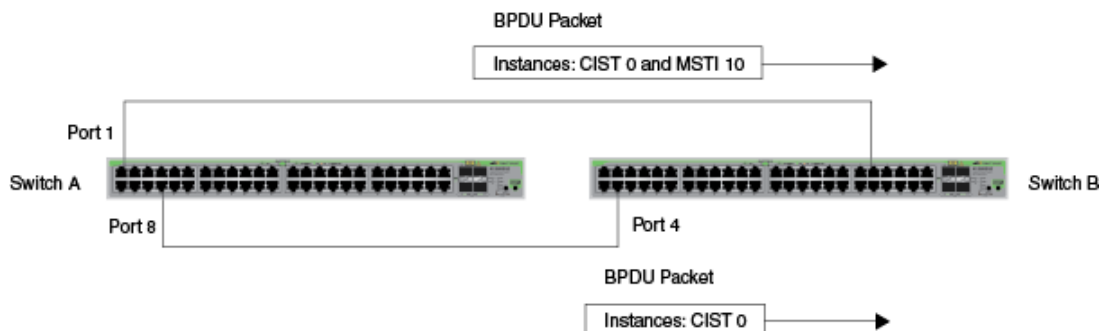
Figure 126. CIST and VLAN Guideline - Example 2

When port 4 on switch B receives a BPDU, the switch notes the port sending the packet belongs only to CIST. Therefore, switch B uses CIST in determining whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block a port to cancel the loop.

To avoid this issue, always assign all VLANs on a switch, including the Default_VLAN, to an MSTI. This guarantees that all ports on the switch have an MSTI ID and that helps to ensure that loop detection is based on MSTI, not CIST.

Connecting VLANs Across Different Regions

Special consideration needs to be taken into account when you connect different MSTP regions or an MSTP region and a single-instance STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANS of your network.

As mentioned previously, only the CIST can span regions. An MSTI cannot. Consequently, you may run into a problem if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree disables by blocking ports.

This is illustrated in Figure 127. The example show two switches, each residing in a different region. Port 7 in switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 6 is a tagged and untagged member of three different VLANs, all associated with MSTI 12.

If both switches were a part of the same region, there would be no problem because the ports reside in different spanning tree instances. However, the switches are part of different regions, and MSTIs do not cross regions. Consequently, the result is that spanning tree would determine that a loop exists between the regions, and Switch B would block a port.
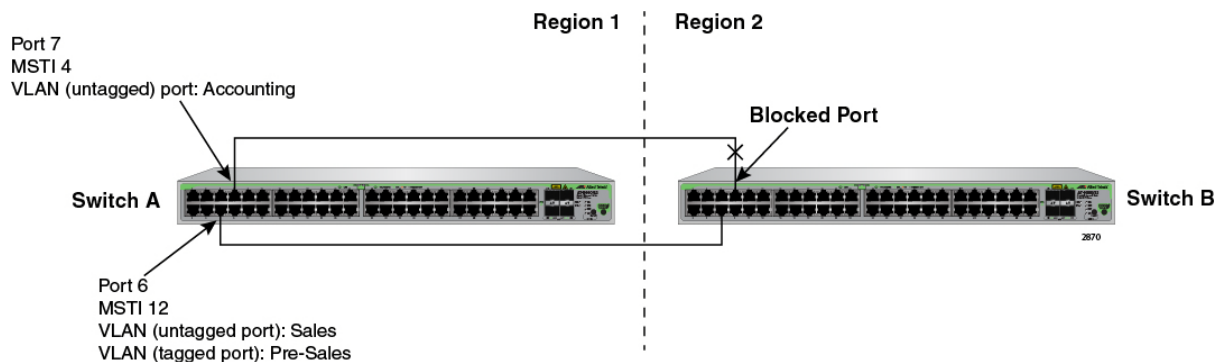
Figure 127. Spanning Regions - Example 1

687

There are several ways to address this issue. The first is to have only *one* MSTP region for each subnet in your network.

Another approach is to group those VLANs that need to span regions into the same MSTI. In this case, VLANs that do not span regions can be assigned to other MSTIs.

Here is an example. Assume that you have two regions that contain the following VLANS:

Table 67. Two Region Examples

Region 1 VLANs	Region 2 VLANs
Sales	Hardware Engineering
Presales	Software Engineering
Marketing	Technical Support
Advertising	Product Management
Technical Support	CAD Development
Product Management	Accounting
Project Management	
Accounting	

The two regions share three VLANs: Technical Support, Product Management, and Accounting. You can group these three VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 11 and in Region 2 you could group them into MSTI 6. After they are grouped, you can connect the VLANs across the regions using a link of untagged/tagged ports. See Figure 128.
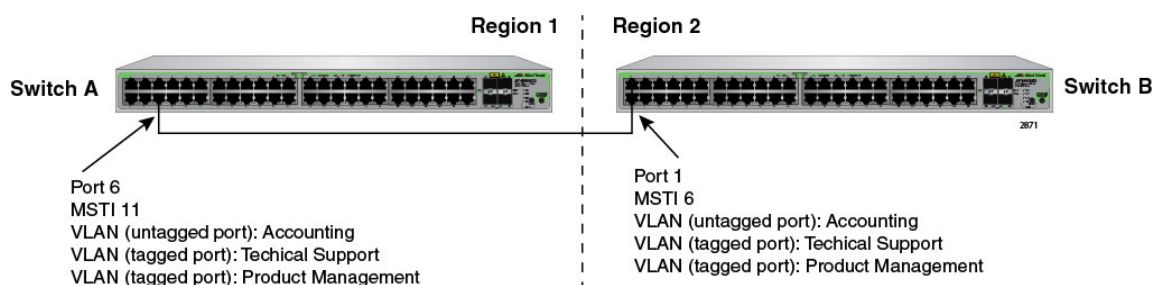
Figure 128. Spanning Regions without Blocking

MSTP Root Guard

The Root Guard feature enforces the root bridge placement in a network. It ensures the port that you have configured with the Root Guard feature is a designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected.

If the bridge receives a superior BPDU on a root-designated port, the Root Guard feature changes the state of the port to a "root inconsistent" STP state. This state varies depending on the spanning tree designation. For MSTP, this is a discarding state. For more information about this command, see "SPANNING-TREE GUARD ROOT" on page 705.

Note
This feature is also supported in STP and RSTP.

Chapter 46
MSTP Commands

The MSTP commands are summarized in Table 68 and described in detail within the chapter.

Table 68. Multiple Spanning Tree Protocol Commands

Command	Mode	Description
"INSTANCE MSTI-ID PRIORITY" on page 693	Interface Configuration	Sets the port priority for an MST instance (MSTI).
"INSTANCE MSTI-ID VLAN" on page 695	MST Configuration	Create an MSTI instance and associate a VLAN with it.
"NO SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 696	Global Configuration	Deactivates the BPDU guard timer.
"NO SPANNING-TREE PORTFAST" on page 697	Port Interface	Removes ports as edge ports on the switch.
"NO SPANNING-TREE MSTP ENABLE" on page 698	Global Configuration	Disables MSTP on the switch.
"SHOW SPANNING-TREE" on page 699	User Exec and Privileged Exec	Displays the MSTP settings on the switch.
"SHOW SPANNING-TREE MST CONFIG" on page 700	Privileged Executive	Displays the MSPT Configuration information for a bridge.
"SHOW SPANNING-TREE MST" on page 701	Privileged Executive	Displays the MST to VLAN port mapping.
"SHOW SPANNING-TREE MST INSTANCE" on page 702	Privileged Executive	Displays detailed information for a particular instance.
"SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 703	Global Configuration	Activates the timer for the BPDU guard feature.
"SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL" on page 704	Global Configuration	Specifies the duration of the BPDU guard timer.
"SPANNING-TREE GUARD ROOT" on page 705	Port Interface	Enables the Root Guard feature on a port.
"SPANNING-TREE MODE MSTP" on page 706	Global Configuration	Sets MSTP as the spanning tree protocol.

Table 68. Multiple Spanning Tree Protocol Commands (Continued)

Command	Mode	Description
"SPANNING-TREE MSTP ENABLE" on page 707	Global Configuration	Designates the MSTP mode on the switch.
"SPANNING-TREE MST CONFIGURATION" on page 708	Global Configuration	Enters the MST Configuration mode.
"SPANNING-TREE MST INSTANCE" on page 709	Interface Configuration	Associates an MSTI with a port.
"SPANNING-TREE PATH-COST" on page 710	Port Interface	Specifies the cost of a port to the root bridge.
"SPANNING-TREE PORTFAST" on page 711	Port Interface	Designates the ports as edge ports.
"SPANNING-TREE PORTFAST BPDU-GUARD" on page 712	Interface Configuration	Enables the Root Guard feature.
"REGION" on page 713	MST Configuration	Assigns a name to an MST region.
"REVISION" on page 714	MST Configuration	Assigns an MST revision number.

INSTANCE MSTI-ID PRIORITY

Syntax

```
instance msti-id priority priority
```

Parameters

priority
Specifies a port priority. The range is 0 to 61440, in increments of 4096.

Mode

Interface Configuration mode

Description

Use this command to set the port priority for an MST instance (MSTI).

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 is chosen as the root port over a port— equivalent in all other aspects— but with a higher priority value. The default value is 32768. For information about MSTI, see "MSTI Guidelines" on page 675.

The range is 0 to 61,440, in increments of 4,096. The range is divided into the sixteen increments listed in Table 69. You specify the increment that represents the bridge priority value you want to assign the switch. The default value is 32,768 (increment 8).

Table 69. MSTP Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344

Table 69. MSTP Bridge Priority Value Increments (Continued)

Increment	Bridge Priority	Increment	Bridge Priority
7	28672	15	61440

Use the no command, NO INSTANCE MSTI-ID PRIORITY, to restore the default priority value of 32768.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example assigns MSTI ID 3 a priority of 4096 to port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mstp enable
awplus(config)# spanning-tree spanning-tree mst
configuration
awplus(config-mst)# interface port 1.0.4
awplus(config-mst)# instance 3 priority 4096
```

694

INSTANCE MSTI-ID VLAN

Syntax

```
instance msti-id vlan vid|vidlist
```

Parameters

vid

Specifies a VLAN ID.

vidlist

Specifies a list of VLAN IDs.

Mode

Port Interface mode

Description

Use this command to permit MSTP to create an instance and associate an instance with one or more VLANs. The switch supports up to 15 MSTIs. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time. For information about MSTI, see "MSTI Guidelines" on page 675.

After you use the INSTANCE MSTI-ID VLAN command to create an instance and associate it with a VLAN, use the SPANNING-TREE MST INSTANCE command to associate ports with each instance. See "SPANNING-TREE MST INSTANCE" on page 709.

Use the no command, NO INSTANCE MSTI-ID VLAN, to delete an instance and its associated VLAN ID.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example assigns an MSTI ID 3 to VLAN 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mstp enable
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 3 vlan 7
```

695

NO SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE

Syntax

```
spanning-tree errdisable-timeout enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to deactivate the timer for the MSTP BPDU guard feature. When the timer is deactivated, ports that the feature disables because they receive BPDU packets remain disabled until you manually activate them again with the NO SHUTDOWN command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example deactivates the timer for the MSTP BPDU guard feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree errdisable-timeout enable
```

NO SPANNING-TREE PORTFAST

Syntax

```
no spanning-tree portfast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove ports as edge ports on the switch. This command is equivalent to "NO SPANNING-TREE PORTFAST" on page 649.

Example

This example removes port 21 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# no spanning-tree portfast
```

NO SPANNING-TREE MSTP ENABLE

Syntax

```
no spanning-tree mstp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable MSTP on the switch.

> **Note**
> Before disabling the spanning tree protocol on the switch, display the MSTP states of the ports and disconnect the network cables from any ports that are in the discarding state. Ports that are in the discarding state begin to forward traffic again when MSTP is disabled. Leaving the cables connected may result in broadcast storms from network loops. To view the states of the ports, refer to "SHOW SPANNING-TREE" on page 699.

Confirmation Command

"SHOW SPANNING-TREE" on page 699

Example

This example disables MSTP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree mstp enable
```

SHOW SPANNING-TREE

Syntax

```
show spanning-tree
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the MSTP settings on the switch. An example of the display is shown in Figure 129.

```
% Default: Bridge up - Spanning Tree Enabled
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% Default: CIST Root Id 8000:eccd6d1e5228
% Default: CIST Reg Root Id 8000:eccd6d1e5228
% Default: CIST Bridge Id 8000:eccd6d1e5228
% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   Instance      VLAN
%   0             1
```

Figure 129. SHOW SPANNING-TREE Command for MSTP

Example

This example displays MSTP settings on the switch:

```
awplus# show spanning-tree
```

SHOW SPANNING-TREE MST CONFIG

Syntax

```
show spanning-tree mst config
```

Parameters

None

Mode

Privileged Executive Mode

Description

Use this command to display the MSTP configuration information for a bridge. Use the display to check that the digest is the same on this device as for all other devices in the same region.

Example

This example displays the MSTP configuration information for a bridge:

```
awplus> enable
awplus# show spanning-tree mst config
```

An example of the display is shown in Figure 130.

```
%
% MSTP Configuration Information for bridge 0:
% ----------------------------------------------------------------
%  Format Id: 0
%  Name:
%  Revision Level: 0
%  Digest: 0xAC36177F50283CD4B83821D8AB26DE62
% ----------------------------------------------------------------
```

Figure 130. SHOW SPANNING-TREE MST CONFIG Command

SHOW SPANNING-TREE MST

Syntax

```
show spanning-tree mst
```

Parameters

None

Mode

Privileged Executive Mode

Description

Use this command to display the MST to VLAN port mapping.

Example

This example displays the MST to VLAN port mappings:

```
awplus> enable
awplus# show spanning-tree mst
```

An example of the display is shown in Figure 131.

```
% Default: Bridge up - Spanning Tree Enabled
% Default: CIST Root Path Cost 200000 - CIST Root Port 33033 - CIST
Bridge Priority 327 68
%  Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 0
%  Default: CIST Root Id 00:30:84:fd:7a:55
%  Default: CIST Reg Root ID 02:10:18:47:04:10
%  Default: CIST Bridge ID 02:10:18:47:04:10
%  Default: CIST 4 topology change(s) - last topology change Sat Jan 1
00:01:35:2000


%  Instance VLAN
%  0: 1,4095
```

Figure 131. SHOW SPANNING-TREE MST Command

SHOW SPANNING-TREE MST INSTANCE

Syntax

```
show spanning-tree mst instance <msti-id>
```

Parameters

instance
> Specifies an instance ID. The range is from 1 to 15.

Mode

Privileged Executive Mode

Description

Use this command to display detailed information for a particular instance and all switch ports associated with that instance.

Example

This example displays detailed information for instance 4 and all the ports associated with that instance:

```
awplus> enable
awplus# show spanning-tree mst instance 4
```

SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE

Syntax

```
spanning-tree errdisable-timeout enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the timer for the BPDU guard feature. The BPDU guard feature prevents unnecessary domain convergences by disabling edge ports if they receive BPDUs. When the timer is activated, the switch will automatically reactivate disabled ports. The time interval that ports remain disabled is set with "SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL" on page 704.

To disable the timer for the BPDU guard feature, use the NO SPANNING-TREE ERRDISABLE TIMEOUT INTERVAL command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

The following example activates the timer for the BPDU guard feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout enable
```

SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL

Syntax

```
spanning-tree errdisable-timeout interval interval
```

Parameters

interval

Specifies the number of seconds that ports remain disabled by the BPDU guard feature. The range is 10 to 1000000 seconds. The default is 300 seconds.

Mode

Global Configuration mode

Description

Use this command to specify the number of seconds that must elapse before the switch automatically enables ports that are disabled by the BPDU guard feature. To activate the timer, refer to "SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 703.

To reset the timer to its default value of 300 seconds, use the NO SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets the time interval to 200 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout interval
200
```

704

SPANNING-TREE GUARD ROOT

Syntax

```
spanning-tree guard root
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable the Root Guard feature on the specified port. The Root Guard feature ensures that the port on which it is enabled is a designated port. If a Root-Guard-enabled port receives a superior BPDU, that may cause it to become a root port, then the port traffic is placed in a "root inconsistent" state. For MSTP, this state is a discarding state.

Use the no version of this command, NO SPANNING-TREE GUARD ROOT, to disable the Root Guard feature on the specified port.

To view the current setting for this parameter, refer to "SHOW SPANNING-TREE" on page 699.

Confirmation Command

"SHOW SPANNING-TREE" on page 699

Examples

This example enables the Root Guard feature on port 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# spanning-tree guard root
```

This example disables the Root Guard feature on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no spanning-tree guard root
```

SPANNING-TREE MODE MSTP

Syntax

```
spanning-tree mode mstp
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to set MSTP as the spanning tree protocol mode.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example sets MSTP as the spanning tree protocol mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
```

SPANNING-TREE MSTP ENABLE

Syntax

```
spanning-tree mstp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to designate MSTP as the active spanning tree protocol on the switch. After activating the protocol, you can enable or disable the spanning tree protocol and set the switch or port parameters.

MSTP is active on the switch only after you have designated it as the active spanning tree with this command and enabled it with "SPANNING-TREE MST CONFIGURATION" on page 708.

Only one spanning tree protocol, STP, RSTP, or MSTP can be active on the switch.

Confirmation Command

"SHOW SPANNING-TREE" on page 699

Example

This example enables MSTP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mstp enable
```

SPANNING-TREE MST CONFIGURATION

Syntax

```
spanning-tree mst configuration
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enter the MST mode.

> **Note**
> Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on the switch.

Confirmation Command

"SHOW SPANNING-TREE" on page 699

Example

This example enters the MST mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mstp mode
awplus(config)# spanning-tree mst configuration
```

SPANNING-TREE MST INSTANCE

Syntax

```
spanning-tree mst instance <1-15>
```

Parameters

instance
Specifies an instance ID. The range is from 1 to 15.

Mode

Interface Configuration mode

Description

Use this command to associate a Multiple Spanning Tree instance (MSTI) with a port. Before you assign an instance ID to a port, you must create an instance. To create an instance, use the INSTANCE MSTI-ID VLAN command. See "INSTANCE MSTI-ID VLAN" on page 695.

Ports are automatically configured to send and receive spanning-tree information for the associated MSTI when you assign a VLAN to the MSTI using the INSTANCE MST-ID VLAN command. For information about this command, see "INSTANCE MSTI-ID VLAN" on page 695.

To remove the association between an MST instance and a port, use the NO SPANNING-TREE MST INSTANCE command. In addition, to disable the automatic configuration of member ports of a VLAN to an associated MSTI, use the NO SPANNING-TREE MST INSTANCE command to remove the member port from the MSTI.

Confirmation Command

"SHOW SPANNING-TREE" on page 699

Example

In the following example, port 2 is associated with instance 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 12
```

SPANNING-TREE PATH-COST

Syntax

```
spanning-tree path-cost path-cost
```

Parameters

path-cost
> Specifies the cost of a port to the root bridge. The range is 1 to 200000000.

Mode

Port Interface mode

Description

Use this command to specify the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. For MSTP, this command only applies to the path cost for CIST. The lower the numeric value, the higher the priority of a path. The range is 1 to 200000000. The default depends on the port speed.

To return a port to the default value, use the no version of this command, NO SPANNING-TREE PATH-COST.

Confirmation Command

"SHOW SPANNING-TREE" on page 699

Example

This example assigns port 2 a port cost of 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 22
```

710

SPANNING-TREE PORTFAST

Syntax

```
spanning-tree portfast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to designate edge ports on the switch. Edge ports are not connected to spanning tree devices or to LANs that have spanning tree devices. As a consequence, edge ports do not receive BPDUs. If an edge port starts to receive BPDUs, it is no longer considered an edge port by the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example configures port 17 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# spanning-tree portfast
```

SPANNING-TREE PORTFAST BPDU-GUARD

Syntax

```
spanning-tree portfast bpdu-guard
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the Root Guard feature on the switch which protects the switch from receiving superior BPDUs.

Use the no version of this command, NO SPANNING-TREE PORTFAST BPDU-GUARD, to disable the root guard feature on a switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example enables the root guard feature on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

712

REGION

Syntax

region *<region-name>*

Parameters

region-name
    Specifies the name of an MST region. Up to 32 characters.

Mode

MSTP Configuration mode

Description

Use this command to name the MSTP Region.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158 or "SHOW SPANNING-TREE" on page 699

Example

This example names the MSTP region "santa clara county:"

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mst enable
awplus(config)# spanning-tree mst configuration
awplus (config-mst)# region santa_clara_county
```

REVISION

Syntax

```
revision <revision-number>
```

Parameters

revision-number
> Specifies the revision number. The range is 0 to 255.

Mode

MST Configuration mode

Description

Use this command to specify the revision number of the current MST configuration. This value is an arbitrary value that you assign to an MST region. Use the revision number to track the number of times an MST configuration has been updated on the network.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

"SHOW SPANNING-TREE" on page 699

Example

This example specifies the MST revision number as 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mst enable
awplus(config)# spanning-tree mst configuration
awplus (config-mst)# revision 4
```

714

Section VII
Virtual LANs

This section contains the following chapters:

716

Chapter 47

Port-based and Tagged VLANs

This chapter covers the following topics:

Overview

A VLAN is a group of ports that form a logical Ethernet segment on an Ethernet switch. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN.

VLANs let you segment your network through the switch's management software so that you can group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

VLANs offer several important benefits:

❒ Improved network performance

Network performance often suffers as networks grow in size and as traffic increases. The more nodes on each LAN segment vying for bandwidth, the greater the likelihood overall network performance will decrease.

VLANs improve network perform because VLAN traffic stays within the VLANs. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them and frees up bandwidth within all the logical workgroups.

In addition, broadcast traffic remains within a VLAN because each VLAN constitutes a separate broadcast domain. This, too, can improve overall network performance.

❒ Increased security

Because network traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, you can use VLANs to control the flow of packets in your network and prevent packets from flowing to unauthorized end nodes.

❒ Simplified network management

VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to be made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment often required a change to the wiring at the switch.

With VLANS, you can use the switch's management software to change the LAN segment assignments of end nodes, without having to physically move workstations or move cables from one switch port to another port.

718

Virtual LANs can also span more than one switch. This makes it possible to create VLANs of end nodes that are connected to switches located in different physical locations.

The switch supports the following types of VLANs you can create yourself:

❒ Port-based VLANs

❒ Tagged VLANs

These VLANs are described in the following sections.

Port-based VLAN Overview

As the "Overview" on page 718 explains, a VLAN consists of a group of ports that form an independent traffic domain on one or more Ethernet switches. Traffic generated by the end nodes remain within their respective VLANs and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on a Gigabit Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A port-based VLAN also can span switches and consist of ports from multiple Ethernet switches.

Note
The switch is pre-configured with one port-based VLAN, called the Default_VLAN. All ports on the switch are members of this VLAN.

The parts that make up a port-based VLAN are:

- □ VLAN name
- □ VLAN Identifier
- □ Untagged ports
- □ Port VLAN Identifier

VLAN Name To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices that are to be members of the VLAN. Examples include Sales, Production, and Engineering.

VLAN Identifier Every VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you assign it a unique VID that is different from all other VLANs in your network.

If a VLAN spans multiple switches, then assign the same VID for the VLAN on the different switches. Then the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

720

For example, if you had a port-based VLAN named Marketing that spanned three switches, assign the Marketing VLAN on each switch the same VID.

You can assign this number manually or allow the management software to do it automatically. If you allow the management software to do it automatically, it selects the next available VID. This is acceptable when you are creating a new, unique VLAN.

If you are creating a VLAN that is part of a larger VLAN that spans several switches, then you need to assign the number yourself so that the VLAN has the same VID on all the switches.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to a port on which a frame is received, and forwards a frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. In addition, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, if you create a port-based VLAN on the switch and assign it a VID of 5, assign the PVID for each port in the VLAN to 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the management software performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is a member, when you assign the port as an untagged member to a VLAN.

Untagged Ports

You need to specify which ports on the switch are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by a port's PVID. (There is another type of VLAN where VLAN membership is determined by information within the frames themselves, rather than by a port's PVID. This type of VLAN is explained in "Tagged VLAN Overview" on page 726.)

A port on the switch can be an untagged member of only one port-based VLAN at a time. An untagged port *cannot* be assigned to two port-based VLANs simultaneously.

Guidelines to Creating a Port-based VLAN

Below are the guidelines to creating a port-based VLAN.

❑ Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiples switches, each part of the VLAN on the different switches should be assigned the same VID.

❑ A port can be an untagged member of only one port-based VLAN at a time.

❑ The PVID of a port is identical to the VID of the VLAN where the port is an untagged member. The PVID value is automatically assigned by the switch.

❑ A port-based VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an interconnection between the switches where the various parts of the VLAN reside.

❑ The switch can support up to a total of 4094 port-based, tagged, protected ports, and MAC address-based VLANs.

❑ A port set to the 802.1x authenticator or supplicant role must be changed to the 802.1x none role before you can change its untagged VLAN assignment. After the VLAN assignment is made, the port's role can be changed back again to authenticator or supplicant, if desired.

❑ You cannot delete the Default VLAN from the switch.

❑ Deleting an untagged port from the Default VLAN without assigning it to another VLAN results in the port being an untagged member of no VLAN.

Drawbacks of Port-based VLANs

There are several drawbacks to port-based VLANs:

❑ It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs. The introduction of a router into your network could create security issues from unauthorized access to your network.

❑ A VLAN that spans several switches requires a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches would require one port on each switch to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports could end up being used ineffectively just to interconnect the various VLANs.

Port-based Example 1

Figure 132 illustrates an example of one AT-9000 switch with three port-based VLANs. (The Default VLAN is not shown in the following examples.)
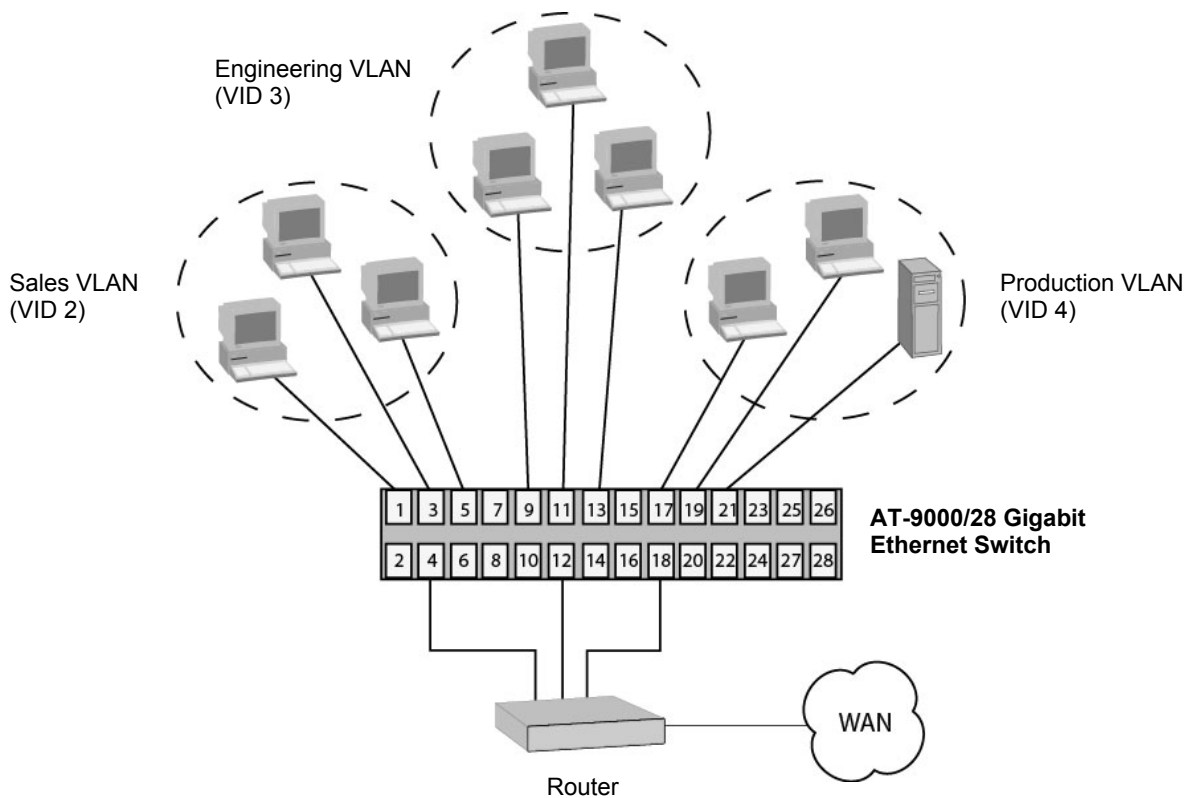
Figure 132. Port-based VLAN - Example 1

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switch.

Switch	Sales VLAN (VID 2)	Engineering VLAN (VID 3)	Production VLAN (VID 4)
AT-9000 Switch	Ports 1, 3 - 5 (PVID 2)	Ports 9, 11 - 13 (PVID 3)	Ports 17 - 19, 21 (PVID 4)

Each VLAN has a unique VID. You assign a VID number when you create a VLAN.

The ports have been assigned PVID values. A port's PVID is assigned automatically by the switch when you create the VLANs. The PVID of a port is the same as the VID in which the port is an untagged member.

In the example, each VLAN has one port connected to the router. The router interconnects the various VLANs and functions as a gateway to the WAN.

723

Port-based Example 2

Figure 133 on page 724 illustrates more port-based VLANs. In this example, two VLANs, Sales and Engineering, span two switches.
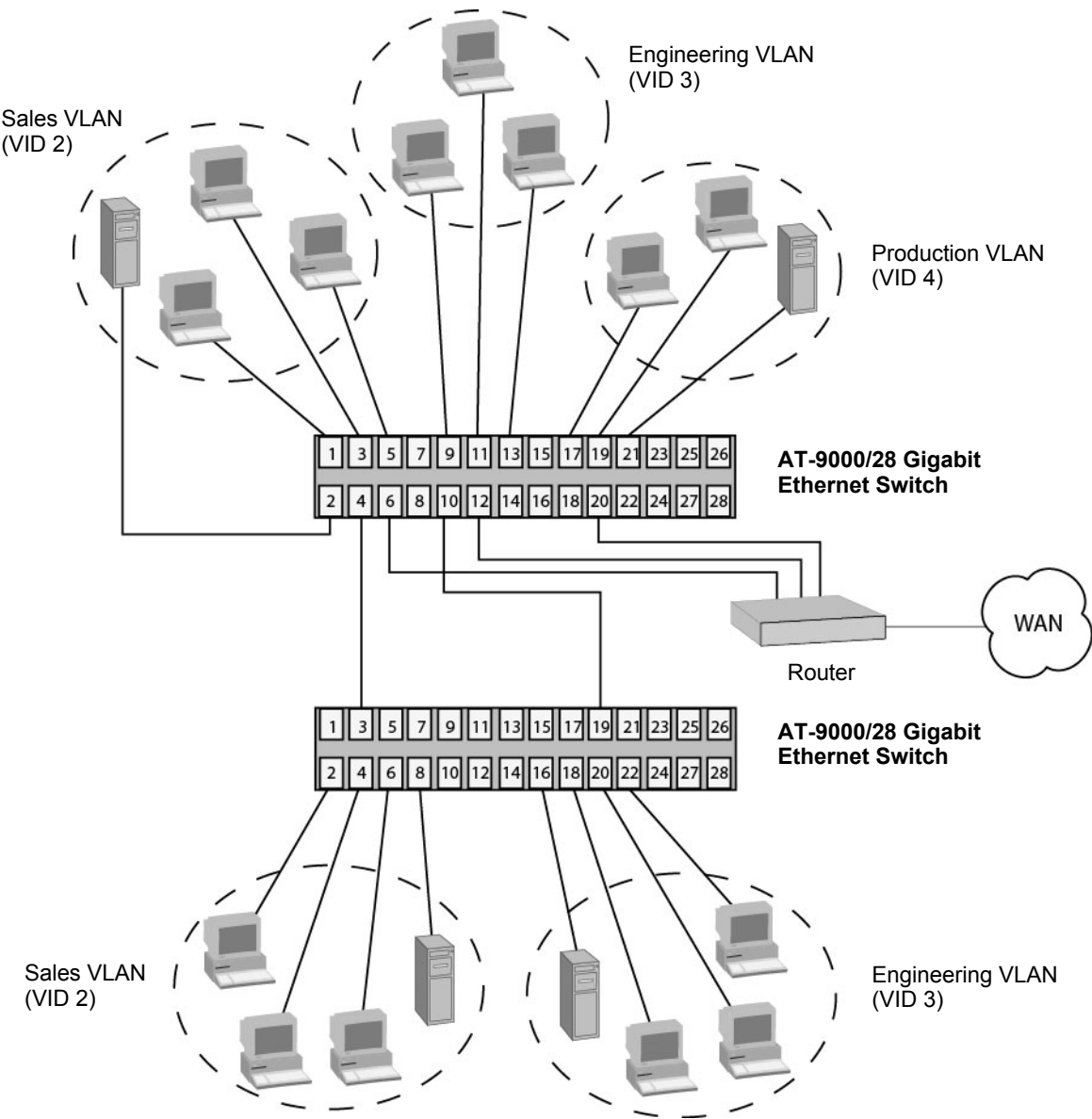
Figure 133. Port-based VLAN - Example 2

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switches:

Switch	Sales VLAN (VID 2)	Engineering VLAN (VID 3)	Production VLAN (VID 4)
AT-9000 Switch (top)	Ports 1 - 6 (PVID 2)	Ports 9 - 13 (PVID 3)	Ports 17, 19 - 21 (PVID 4)
AT-9000 Switch (bottom)	Ports 2 - 4, 6, 8 (PVID 2)	Ports 16, 18-20, 22 (PVID 3)	none

❐ Sales VLAN - This VLAN spans both switches. It has a VID value of 2 and consists of six untagged ports on the top switch and five untagged ports on the bottom switch.

The two parts of the VLAN are connected by a direct link from port 4 on the top switch to port 3 on the bottom switch. This direct link allows the two parts of the Sales VLAN to function as one logical LAN segment.

Port 6 on the top switch connects to the router. This port allows the Sales VLAN to exchange Ethernet frames with the other VLANs and to access the WAN.

❐ Engineering VLAN - The workstations of this VLAN are connected to ports 9 to 13 on the top switch and ports 16, 18 to 20, and 22 on the bottom switch.

Because this VLAN spans multiple switches, it needs a direct connection between its various parts to provide a communications path. This is provided in the example with a direct connection from port 10 on the top switch to port 19 on the bottom switch.

This VLAN uses port 12 on the top switch as a connection to the router and the WAN.

❐ Production VLAN - This is the final VLAN in the example. It has the VLAN of 4, and its ports have been assigned the PVID also of 4.

The nodes of this VLAN are connected only to the top switch. So this VLAN does not require a direct connection to the bottom switch. However, it uses port 20 as a connection to the router.

Tagged VLAN Overview

The second type of VLAN is the tagged VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). As explained earlier in this chapter in "VLAN Identifier" on page 720, this number uniquely identifies each VLAN in a network.

When the switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port to receive or transmit tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1q compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that the tagged ports can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch to connect all VLANs on the switch to another switch.

The IEEE 802.1q standard describes how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN of which the port is a tagged member, the frame is accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame is discarded.

The parts of a tagged VLAN are similar to those for a port-based VLAN. They are:

- ❑ VLAN Name
- ❑ VLAN Identifier
- ❑ Tagged and Untagged Ports
- ❑ Port VLAN Identifier

Note
For explanations of VLAN name and VLAN identifier, refer back to "VLAN Name" on page 720 and "VLAN Identifier" on page 720.

Tagged and Untagged Ports

You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which are untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs simultaneously.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the PVID of a port determines the VLAN where the port is an untagged member.

Because a tagged port determines VLAN membership by examining the tagged header within the frames that it receives and not the PVID, you might conclude that there is no need for a PVID. However, the PVID is used if a tagged port receives an untagged frame— a frame without any tagged information. The port forwards the frame based on the port's PVID. This is only in cases where an untagged frame arrives on a tagged port. Otherwise, the PVID on a tagged port is ignored.

Guidelines to Creating a Tagged VLAN

Below are the guidelines to creating a tagged VLAN.

❒ Each tagged VLAN must have a unique VID. If a VLAN spans multiple switches, each part of the VLAN on the different switches must have the same VID.

❒ A tagged port can be a member of multiple VLANs.

❒ An untagged port can be an untagged member of only one VLAN at a time.

❒ The switch can support up to a total of 4094 port-based, tagged, protected ports, and MAC address-based VLANs.

Tagged VLAN Example

Figure 134 illustrates how tagged ports can be used to interconnect IEEE 802.1q based products.
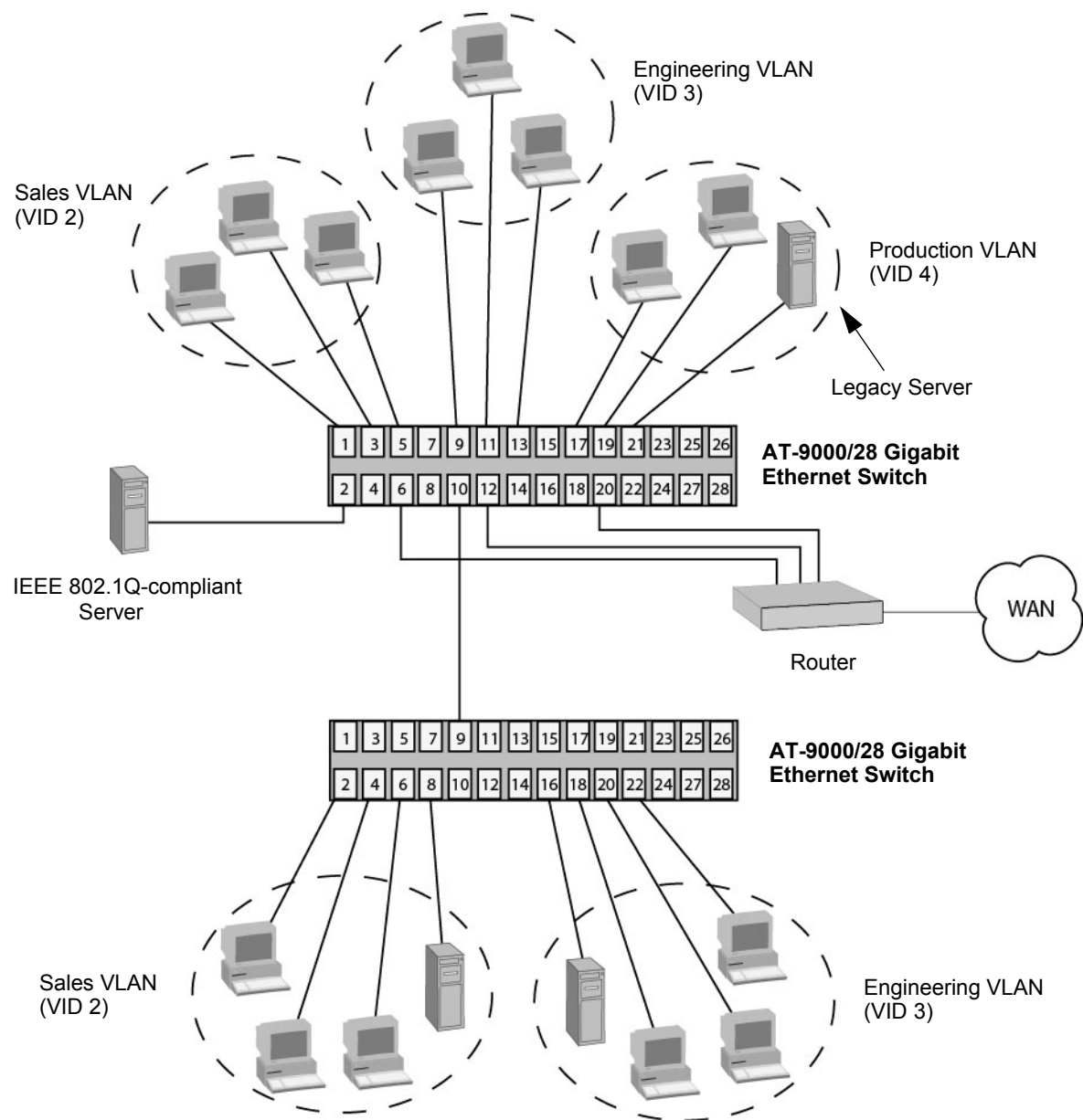
Figure 134. Example of a Tagged VLAN

The port assignments for the VLANs are described in Table 70.

Table 70. VLAN Port Assignments

Switch	Sales VLAN (VID 2)		Engineering VLAN (VID 3)		Production VLAN (VID 4)	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-9000 Switch (top)	1, 3 to 5 (PVID 2)	2, 10	9, 11 to 13 (PVID 3)	2, 10	17, 19 to 21 (PVID 4)	2
AT-9000 Switch (bottom)	2, 4, 6, 8 (PVID 2)	9	16, 18, 20, 22 (PVID 3)	9	none	none

This example is nearly identical to the "Port-based Example 2" on page 724. Tagged ports have been added to simplify network implementation and management.

One of the tagged ports is port 2 on the top switch. This port has been made a tagged member of the three VLANs. It is connected to an IEEE 802.1q compliant server, meaning the server can handle frames from multiple VLANs. Now all three VLANs can access the server without going through a router or other interconnection device.

It is important to note that even though the server is accepting frames from and transmitting frames to more than one VLAN, data separation and security remain.

Two other tagged ports are used to simplify network design in the example. They are port 10 on the top switch and port 9 on the lower switch. These ports have been made tagged members of the Sales and Engineering VLANs so that they can carry traffic from both VLANs, simultaneously. These ports provide a common connection that enables different parts of the same VLAN to communicate with each other while maintaining data separation between VLANs.

In comparison, the Sales and Engineering VLANs in the "Port-based Example 2" on page 724 each had to have its own individual network link between the switches to connect the different parts of the VLANs. But with tagged ports, you can use one data link to carry data traffic from several VLANs, while still maintaining data separation and security. The tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the tagged frame originated.

Creating VLANs

To create VLANs, use the VLAN command in the VLAN Configuration mode. You must specify a name and a VID for a new VLAN in the command. A name can have up to 20 characters. Giving the VLANs unique names make them easier to identify.

A new VLAN also needs a VID number, which has a range of 2 to 4094. (The VID 1 is reserved for the Default_VLAN.) Each VLAN on the switch must be assigned a unique VID. VLANs that span more than one switch should be assigned the same VID number on each switch.

Here is the format of the command:

vlan *vid* [name *name*]

This example creates the Engineering VLAN and assigns it a VID of 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 5 name Engineering
```

> **Note**
> The VLAN name field is used only as a description in the SHOW VLAN command output. It cannot be a substituted for the VID when specifying a specific VLAN in other commands.

This example creates four new VLANs that have the VIDs of 4, 5, 6 and 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 4-6,11
```

> **Note**
> You cannot specify a name when creating more than one VLAN.

New VLANs do not have any ports. To add untagged ports, refer to "Adding Untagged Ports to VLANs" on page 732. To add tagged ports, refer to "Adding Tagged Ports to VLANs" on page 734.

Adding Untagged Ports to VLANs

To add a port to a VLAN as an untagged port, it may be necessary to first set its mode with the SWITCHPORT MODE ACCESS command in the Port Interface mode. Once a port's mode is set to access, it functions as an untagged port. However, this step may not be necessary because the default mode setting for all ports is as untagged ports. In fact, the only situation where you are likely to use the command is on ports that need to function as untagged ports again after acting as tagged ports. Here is the format of the command:

```
switchport mode access [ingress-filter enable|disable]
```

For an explanation of the INGRESS-FILTER parameter, refer to "SWITCHPORT MODE ACCESS" on page 750.

After you've set the mode of a port to access (or if it is already set to that mode), you can use the SWITCHPORT ACCESS VLAN command, which is also found in the Port Interface mode, to assign it as an untagged member of a VLAN. Here is the format of the command:

```
switchport access vlan vid
```

The VID parameter is the VLAN to which you want to add the untagged port. If you do not know the number, use the SHOW VLAN ALL command in the User Exec mode or the Privileged Exec mode to view the VLANs on the switch. You can specify just one VID in the command because a port can be an untagged member of just one VLAN at a time. The designated VLAN must already exist on the switch.

This example of the commands designates ports 5 and 7 as untagged ports and adds them to a VLAN with the VID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.7
awplus(config-if)# switchport mode access
awplus(config-if)# switchport access vlan 12
```

When the switch adds the ports to VLAN 12, it removes them from their current VLAN assignments because a port can be an untagged member of just one VLAN at a time.

This example designates ports 11 to 18 as untagged ports of a VLAN with the VID 4. The SWITCHPORT MODE ACCESS command is omitted because the example assumes the ports are already designated as untagged ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.18
awplus(config-if)# switchport access vlan 4
```

Adding Tagged Ports to VLANs

There are three steps to adding ports as tagged ports to VLANs:

1. Set the mode of the ports to trunk so that they function as tagged ports. This is performed with the SWITCHPORT MODE TRUNK command.

2. Assign the ports to VLANs with the SWITCHPORT TRUNK ALLOWED VLAN command.

3. Specify the VLAN for untagged ingress packets. This VLAN is referred to as the native VLAN. The command is the SWITCHPORT TRUNK NATIVE VLAN command.

You cannot add a port as a tagged member to a VLAN until after you set its VLAN mode to trunk with the SWITCHPORT MODE TRUNK command. Afterwards, you can assign it as a tagged port to as many VLANs as you want. The command has the format shown here:

```
switchport mode trunk [ingress-filter enable/disable]
```

For an explanation of the optional INGRESS-FILTER parameter, refer to "SWITCHPORT MODE TRUNK" on page 751.

Once a port is labeled as a tagged port, you can add it to VLANs as a tagged member with the SWITCHPORT TRUNK ALLOWED VLAN command. The command has this format:

```
switchport trunk allowed vlan add vid
```

The VID parameter is the ID number of the VLAN to which you want to add the port as a tagged port. You can specify more than one VLAN because tagged ports can belong to more than one VLAN at a time. The VLANs must already exist on the switch.

Both of these commands are located in the Port Interface mode.

This example of the commands adds port 23 as a tagged member to a VLAN with the VID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 5
```

734

This example adds ports 18 to 21 as tagged members to VLANs with the VIDs 7 and 13:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18-port1.0.21
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 7,13
```

Although tagged ports are primarily intended to handle tagged packets, they may also handle untagged packets. These are packets that do not have any VLAN IDs. To forward these types of packets, tagged ports need to be able to assign them to a particular VLAN on the switch.

This is controlled with what is called native VLANs. A native VLAN is simply the ID number of a VLAN to which a tagged port assigns its ingress untagged frames. For example, a tagged VLAN that is assigned the native VLAN 12 assigns all ingress untagged packets to that VLAN and forwards the packet on to ports in that particular VLAN. A port can have only one native VLAN.

The command for setting the native VLAN of tagged ports is the SWITCHPORT TRUNK NATIVE VLAN command, in the Port Interface mode. Here is the command's format:

```
switchport trunk native vlan vid
```

The VID parameter is the ID number of the VLAN that is to be the native VLAN of the untagged port. You can specify just one VID because a tagged port can have just one native VLAN. The VLAN must already exist on the switch.

This example adds ports 22 and 23 as tagged members to VLANs with the VIDs 8 and 9. The example designates the native VLAN for ingress untagged packets on the ports as VLAN 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22-port1.0.23
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 8,9
awplus(config-if)# switchport trunk native vlan 15
```

This example changes the native VLAN of port 16 to VLAN 23. The example assumes that the port is already a tagged port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# switchport trunk native vlan 23
```

Removing Untagged Ports from VLANs

To remove untagged ports from their current VLAN assignments and return them back to the Default VLAN, use the NO SWITCHPORT ACCESS VLAN command in the Port Interface mode. You do not specify a VLAN ID number in the command because a port can be an untagged member of just one VLAN at a time. The switch removes the designated port from whichever VLAN it is an untagged member and returns it back to the Default_VLAN.

You can remove more than one port at a time from a VLAN, and the same command can be used to remove untagged ports from different VLANs.

This example removes untagged port 5 from its current VLAN assignment and returns it to the Default_VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no switchport access vlan
```

This example removes untagged ports 10 to 14 from their current VLAN assignments and returns them to the Default_VLAN. This example works even if the ports are untagged members of different VLANs.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.10-port1.0.14
awplus(config-if)# no switchport access vlan
```

736

Removing Tagged Ports from VLANs

Use the SWITCHPORT TRUNK ALLOWED VLAN command to remove ports as tagged members from VLANs. This command is actually used for both adding and removing tagged ports. The format of the command when it is used to remove ports is shown here:

```
switchport trunk allowed vlan none|remove vid
```

To remove a port from all its tagged VLAN assignments, use the NONE parameter. Otherwise, use the REMOVE parameter and enter the ID numbers of the VLANs from which the port is to be removed.

This example removes tagged ports 18 and 19 from the VLAN with the VID 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.19
awplus(config-if)# switchport trunk allowed vlan remove 7
```

If, after removing a port from all its tagged VLAN assignments, you do not want it to function as a tagged port on the switch, use the NO SWITCHPORT TRUNK command to remove the trunk mode. This example removes ports 8 and 12 as tagged members from all their VLAN assignments and removes the trunk mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8,port1.0.12
awplus(config-if)# switchport trunk allowed vlan none
awplus(config-if)# no switchport trunk
```

Deleting VLANs

To delete VLANs from the switch, use the NO VLAN command in the VLAN Configuration mode. You cannot delete the Default_VLAN. The untagged ports of deleted VLANs are automatically returned back to the Default_VLAN. Here is the format of the command:

```
no vlan vid
```

This example deletes the VLAN with the VID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 12
```

Displaying the VLANs

To display the VLANs on the switch, use the SHOW VLAN ALL command in the User Exec mode and Privileged Exec mode:

```
awplus# show vlan all
```

An example of the information is shown in Figure 135.

```
VLAN ID   Name       Type      State     Member ports
                                         (u)-Untagged, (t) Tagged
=======   =======    =======   =======   ==========================
1         default    STATIC    ACTIVE    1(u) 20(u) 21(u) 22(u) 23(u)
                                         26(u) 27(u) 28(u)
5         Sales      STATIC    ACTIVE    11(u) 12(u) 13(u) 14(u) 24(u)
                                         25(u)
5         Engineering STATIC   ACTIVE    2(u) 3(u) 4(u) 5(u) 6(u) 7(u)
                                         8(u) 15(u) 16(u) 17(u) 25(t)
18        Marketing  STATIC    ACTIVE    9(u) 10(u) 18(u) 19(u) 25(t)
```

Figure 135. SHOW VLAN ALL Command

The information is described in Table 72 on page 746.

Chapter 48

Port-based and Tagged VLAN Commands

The VLAN commands are summarized in Table 71 and described in detail within the chapter.

Table 71. Port-based and Tagged VLAN Commands

Command	Mode	Description
"NO SWITCHPORT ACCESS VLAN" on page 742	Port Interface	Removes untagged ports from VLANs.
"NO SWITCHPORT TRUNK" on page 743	Port Interface	Removes the tagged designation from ports.
"NO SWITCHPORT TRUNK NATIVE VLAN" on page 744	Port Interface	Reestablishes the Default_VLAN as the native VLAN of tagged ports.
"NO VLAN" on page 745	VLAN Configuration	Deletes VLANs from the switch.
"SHOW VLAN" on page 746	User Exec and Privileged Exec	Displays all the VLANs on the switch.
"SWITCHPORT ACCESS VLAN" on page 748	Port Interface	Adds untagged ports to a VLAN.
"SWITCHPORT MODE ACCESS" on page 750	Port Interface	Designates ports as untagged ports.
"SWITCHPORT MODE TRUNK" on page 751	Port Interface	Designates ports as tagged ports.
"SWITCHPORT TRUNK ALLOWED VLAN" on page 753	Port Interface	Adds and removes tagged ports from VLANs.
"SWITCHPORT TRUNK NATIVE VLAN" on page 756	Port Interface	Designates native VLANs for tagged ports.
"VLAN" on page 758	VLAN Configuration	Creates VLANs.

741

NO SWITCHPORT ACCESS VLAN

Syntax

```
no switchport access vlan
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to return untagged ports to the Default_VLAN.

Note

You cannot return ports to the Default_VLAN if they are set to the authenticator role for 802.1x port-based network access control. You must first remove the authenticator role. For instructions, refer to "NO DOT1X PORT-CONTROL" on page 950.

Confirmation Command

"SHOW VLAN" on page 746

Example

This example removes untagged port 5 from its current VLAN assignment and returns it to the Default VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no switchport access vlan
```

NO SWITCHPORT TRUNK

Syntax

```
no switchport trunk
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove the trunk mode from ports. Ports cannot be assigned as tagged ports to VLANs once the trunk mode has been removed.

> **Note**
> You must first remove a port from all tagged VLAN assignments before you can remove its tagged designation. For instructions, refer to "SWITCHPORT TRUNK ALLOWED VLAN" on page 753.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example removes the trunk mode from ports 23 and 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23-port1.0.24
awplus(config-if)# no switchport trunk
```

NO SWITCHPORT TRUNK NATIVE VLAN

Syntax

```
no switchport trunk native vlan
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to reestablish the Default_VLAN as the native VLAN of tagged ports. The native VLAN of a tagged port specifies the appropriate VLAN for ingress and egress untagged packets. A tagged port can have only one native VLAN.

Note

This command will not work if the tagged port is already a tagged member of the Default_VLAN because a port cannot be both a tagged and untagged member of the same VLAN.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example reestablishes the Default_VLAN as the native VLAN for tagged ports 18 and 19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.19
awplus(config-if)# no switchport trunk native vlan
```

744

NO VLAN

Syntax

```
no vlan vid
```

Parameters

vid

>   Specifies the VID of the VLAN you want to delete.

Mode

VLAN Configuration mode

Description

Use this command to delete port-based or tagged VLANs from the switch. Here are the guidelines to this command:

> ❒ You cannot delete the Default_VLAN.
>
> ❒ The switch automatically returns the untagged ports of a deleted VLAN to the Default_VLAN, as untagged ports.
>
> ❒ Static addresses assigned to the ports of a deleted VLAN become obsolete and should be deleted from the MAC address table. For instructions, refer to "NO MAC ADDRESS-TABLE STATIC" on page 360.
>
> ❒ To delete a VLAN that has authenticator or supplicant ports for 802.1x port-based network access control, you must first change the ports to the 802.1x none role. For instructions, refer to "NO DOT1X PORT-CONTROL" on page 950.

Confirmation Command

"SHOW VLAN" on page 746

Example

This example deletes the VLAN with the VID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 5
```

SHOW VLAN

Syntax

```
show vlan vid |all
```

Parameters

vid
> Specifies the VID of the VLAN you want to display.

all
> Specifies all the VLANs on the switch to display.

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display all the tagged and untagged VLANs on the switch. An example of the information is shown in Figure 136.

```
VLAN ID   Name        Type      State     Member ports
                                          (u)-Untagged, (t) Tagged
=======   =======     =======   =======   ============================
1         default     STATIC    ACTIVE    1(u) 20(u) 21(u) 22(u) 23(u)
                                          26(u) 27(u) 28(u)
5         Sales       STATIC    ACTIVE    11(u) 12(u) 13(u) 14(u) 24(u)
                                          25(u)
5         Engineering STATIC    ACTIVE    2(u) 3(u) 4(u) 5(u) 6(u) 7(u)
                                          8(u) 15(u) 16(u) 17(u) 25(t)
18        Marketing   STATIC    ACTIVE    9(u) 10(u) 18(u) 19(u) 25(t)
```

Figure 136. SHOW VLAN Command

The columns in the table are described here:

Table 72. SHOW VLAN Command

Parameter	Description
VLAN ID	The ID numbers of the VLANs.
VLAN name	The names of the VLANs.
Type	The VLAN type, which is either Port Based for port-based and tagged VLANs or DYNAMIC for VLANs created by GVRP.

Table 72. SHOW VLAN Command (Continued)

Parameter	Description
State	The states of the VLANs. A VLAN has an Active state if it has at least one tagged or untagged port and an Inactive state if it does not have any ports.
Member Ports	The untagged (u) and tagged (t) ports of the VLANs.

Example

The following example displays the tagged and untagged VLANs on the switch:

```
awplus# show vlan
```

SWITCHPORT ACCESS VLAN

Syntax

`switchport access vlan `*`vid`*

Parameters

vid

    Specifies the ID number of the VLAN to which you want to add untagged ports. You can specify only one VID.

Mode

Port Interface mode

Description

Use this command to add untagged ports to VLANs. Please review the following information before using this command:

- ❐ The specified VLAN must already exist.
- ❐ A port can be an untagged member of only one VLAN at a time. When you add a port to a VLAN as an untagged member, the switch automatically removes it from its current untagged VLAN assignment before moving it to its new assignment. For example, if you add port 4 as an untagged port to a VLAN, the switch automatically removes the port from the VLAN in which it is currently an untagged member.
- ❐ The PVID of an untagged port is automatically changed to match the VID number of the VLAN where it is added. For instance, if you add port 4 as an untagged member of a VLAN with a VID of 15, the PVID for port 4 is automatically changed to 15.
- ❐ If the ports are configured as authenticator or supplicant ports for 802.1x port-based network access control, you must change the ports to the 802.1x none role before you can change their VLAN assignments.

Confirmation Command

"SHOW VLAN" on page 746

748

Examples

This example adds ports 5 and 7 as untagged ports to a VLAN with the VID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.7
awplus(config-if)# switchport access vlan 12
```

This example returns port 15 as an untagged port to the Default_VLAN, which has the VID 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# switchport access vlan 1
```

Returning ports to the Default_VLAN can also be accomplished with the NO SWITCHPORT ACCESS VLAN. See "NO SWITCHPORT ACCESS VLAN" on page 742.

SWITCHPORT MODE ACCESS

Syntax

```
switchport mode access [ingress-filter enable|disable]
```

Parameters

enable
> Activates ingress filtering.

disable
> Disables ingress filtering.

Mode

Port Interface mode

Description

Use this command to designate ports as untagged ports. This is the first command to adding ports as untagged ports to VLANs. The second command is "SWITCHPORT ACCESS VLAN" on page 748.

The access mode is the default setting for all ports on the switch. Consequently, you only need to perform this command for ports that were changed to the trunk mode for tagged packets and now need to be returned to the access mode for untagged packets.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example designates ports 17 to 24 as untagged ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17-port1.0.24
awplus(config-if)# switchport mode access
```

SWITCHPORT MODE TRUNK

Syntax

```
switchport mode trunk [ingress-filter enable|disable]
```

Parameters

enable

Activates ingress filtering so the tagged port accepts only tagged packets that have one of its tagged VIDs.

disable

Disables ingress filtering so the tagged port accepts all tagged packets.

Mode

Port Interface mode

Description

Use this command to label ports as tagged ports. This is the first command to adding ports as tagged ports to VLANs. The second command is "SWITCHPORT TRUNK ALLOWED VLAN" on page 753.

The INGRESS-FILTER parameter controls whether the tagged port accepts or rejects tagged packets containing VIDs that do not match any of its tagged VIDs. If ingress filtering is enabled, any frame received on the 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. If ingress filtering is disabled, the tagged port accepts all tagged packets.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example designates ports 4 to 6 as tagged ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4-port1.0.6
awplus(config-if)# switchport mode trunk
```

This example designates port 18 as a tagged port and disables ingress filtering so that it accepts all tagged packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18
awplus(config-if)# switchport mode trunk ingress-filter
disable
```

SWITCHPORT TRUNK ALLOWED VLAN

Syntaxes for Adding Tagged Ports to VLANs

```
switchport trunk allowed vlan all
```

```
switchport trunk allowed vlan add vid
```

```
switchport trunk allowed vlan except vid
```

Syntaxes for Removing Tagged Ports from VLANs

```
switchport trunk allowed vlan remove vid
```

```
switchport trunk allowed vlan none
```

Parameters

vlan all
> Adds the port as a tagged port to all the VLANs on the switch.

add vid
> Adds the port as a tagged port to the designated VLAN. You can specify more than one VID.

except vid
> Adds the port as a tagged port to all the VLANs on the switch, except for the designated VLAN. You can specify more than one VID.

remove vid
> Removes the port as a tagged port from the designated VLAN. You can specify more than one VID.

none
> Removes the port as a tagged port from all its tagged VLAN assignments.

Mode

Port Interface mode

Description

Use this command to add tagged ports to VLANs or to remove tagged ports from VLANs. Here are the guidelines to adding tagged ports:

❒ You must designate ports as tagged ports before you can add them to VLANs. The command for designating tagged ports is "SWITCHPORT MODE TRUNK" on page 751.

❏ Ports can be tagged members of more than one VLAN at a time.

❏ The specified VLANs must already exist. To create VLANs, see "VLAN" on page 758.

❏ Adding a port as a tagged member of a VLAN does not change its other tagged and untagged VLAN assignments, because ports can be tagged members of more than one VLAN at a time. For instance, if you add port 6 as a tagged port to a new VLAN, there is no change to the port's other tagged and untagged VLAN memberships.

Here are the guidelines to removing tagged ports from VLANs:

❏ Removing a tagged port from a VLAN does not change any of its other tagged and untagged VLAN assignments.

❏ Ports that are set to the authenticator or supplicant role for 802.1x port-based network access control must be changed to the 802.1x none role before they can be removed from a VLAN. You can reassign their roles after you change their VLAN assignments.

Confirmation Command

"SHOW VLAN" on page 746

Examples of Adding Tagged Ports to VLANs

This example designates port 5 as a tagged port and adds it to the VLAN with a VID of 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 22
```

This example designates ports 18 to 21 as tagged ports and adds them to the VLANs with VIDs of 7 and 9:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18-port1.0.21
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 7,9
```

This example adds port 15 as a tagged port to all the VLANs. It assumes that the port is already designated as a tagged port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# switchport trunk allowed vlan all
```

This example adds ports 22 to 24 as tagged ports to all the VLANs, except for the VLAN with a VID of 11. The example assumes that the ports are already designated as tagged ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22-port1.0.24
awplus(config-if)# switchport trunk allowed vlan except 11
```

Examples of Removing Tagged Ports from VLANs

This example removes tagged port 17 from the VLAN with a VID of 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# switchport trunk allowed vlan remove 8
```

This example removes ports 19 and 22 from all their tagged VLAN assignments:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.19,port1.0.22
awplus(config-if)# switchport trunk allowed vlan none
```

SWITCHPORT TRUNK NATIVE VLAN

Syntax

```
switchport trunk native vlan vid|none
```

Parameters

vid

> Specifies the VID of the VLAN that will act as the default VLAN for all ingress and egress untagged packets on the tagged port. You can enter just one VID.

none

> Reestablishes the Default_VLAN as the native VLAN of the port. This is equivalent to the NO form of this command.

Mode

Port Interface mode

Description

Use this command to designate native VLANs for tagged ports. The native VLAN of a tagged port specifies the appropriate VLAN for ingress untagged packets. A tagged port can have only one native VLAN, and the VLAN must already exist on the switch.

> **Note**
> You cannot assign a native VLAN to a port that is already a tagged member of that VLAN because a port cannot be both a tagged and untagged member of the same VLAN.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example designates VLAN 17 as the native VLAN for tagged port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk native vlan 17
```

This example reestablishes the Default_VLAN as the native VLAN for tagged ports 18 and 20:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.20
awplus(config-if)# switchport trunk native vlan none
```

VLAN

Syntax

vlan *vid* [name *name*]

Parameters

vid

> Specifies a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch. You can specify more than one VID to create more than one VLAN at a time.

> If this VLAN will be unique in your network, its VID should also be unique. If this VLAN will be part of a larger VLAN that spans multiple switches, the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you should assign the Sales VLAN on each switch the same VID value.

name

> Specifies a name for a new VLAN. A name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. VLANs will be easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). A name cannot be the same as a name of an existing VLAN on the switch. If a VLAN is unique in your network, then its name should be unique as well. A VLAN that spans multiple switches should have the same name on each switch.

> If you are creating more than one VLAN, do not include this parameter.

Note
The VLAN name field is used only as a description in the SHOW VLAN command output. It cannot be a substituted for the VID when specifying a specific VLAN in other commands.

Mode

VLAN Configuration mode

758

Description

Use this command to create port-based and tagged VLANs. You can create just one VLAN at a time.

Confirmation Command

"SHOW VLAN" on page 746

Examples

This example creates a new VLAN with the VID 5 and the name Engineering:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 5 name Engineering
```

This example creates a new VLAN with the VID 17 and the name Manufacturing:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 17 name Manufacturing
```

This example creates new VLANs with the VIDs 6 to 11, 15 and 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 6-11,15,23
```

760

Chapter 49

GARP VLAN Registration Protocol

This chapter covers the following topics:

- ❒ "Overview" on page 762
- ❒ "Guidelines" on page 765
- ❒ "GVRP and Network Security" on page 766
- ❒ "GVRP-inactive Intermediate Switches" on page 767
- ❒ "Enabling GVRP on the Switch" on page 768
- ❒ "Enabling GIP on the Switch" on page 769
- ❒ "Enabling GVRP on the Ports" on page 770
- ❒ "Setting the GVRP Timers" on page 771
- ❒ "Disabling GVRP Timers on the Switch" on page 772
- ❒ "Disabling GVRP on the Ports" on page 773
- ❒ "Disabling GIP on the Switch" on page 774
- ❒ "Disabling GVRP on the Switch" on page 775
- ❒ "Restoring the GVRP Default Settings" on page 776
- ❒ "Displaying GVRP" on page 777

Overview

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches. With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

The switch uses GVRP protocol data units (PDUs) to share VLAN information among GVRP-active devices. The PDUs contain the VID numbers of all the VLANs on the switch.

When the switch receives a GVRP PDU on a port, it examines the PDU to determine the VIDs of the VLANs on the device that sent it. It then does the following:

❒ If the PDU contains a VID of a VLAN that does not exist on the switch, it creates the designated VLAN and adds the port that received the PDU as a tagged member of the VLAN. A VLAN created by GVRP is called a dynamic GVRP VLAN.

❒ If the PDU contains a VID of a VLAN that already exists on the switch but the port is not a member of it, the switch adds the port as a tagged member of the VLAN. A port that has been added by GVRP to a static VLAN (that is a user-created VLAN) is called a dynamic GVRP port.

Only GVRP can modify or delete dynamic GVRP VLANs. Dynamic GVRP VLANs exist only if there are active nodes in the VLANs. If all nodes of a dynamic GVRP VLAN are shut down, and there are no active links, GVRP deletes it from the switch.

A dynamic GVRP port in a static VLAN remains a member of the VLAN as long as there are active VLAN members. If all members of the VLAN become inactive or there are no active links, GVRP removes the dynamic port from the VLAN, but does not delete the VLAN if the VLAN is a static VLAN.

762

Figure 137 provides an example of how GVRP works.

Port 1

Switch #1
Static VLAN
Sales VID 11

Port 4

Switch #3
Static VLAN
Sales VID 11

Port 3

Switch #2

Port 2
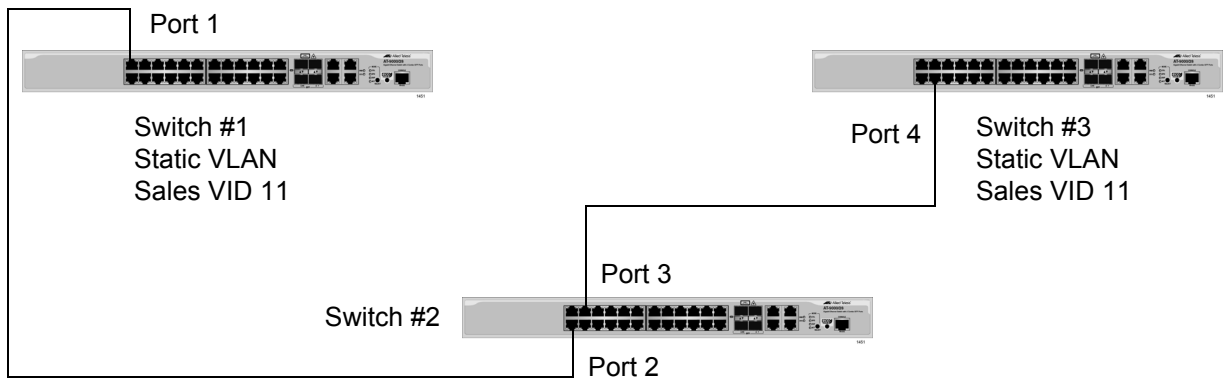
Figure 137. GVRP Example

The example consists of three switches. Switches #1 and #3 have the Sales VLAN, but switch #2 does not. Consequently, the end nodes of the two parts of the Sales VLANs cannot communicate with each other.

Without GVRP, you would have to manually add the Sales VLAN to switch #2. But with GVRP, the VLAN is added automatically. Here is how GVRP would resolve the problem in the example.

1. Port 1 on switch #1 sends to port 2 on switch #2 a PDU that contains the VIDs of all the VLANs on the switch, including VID 11 for the Sales VLAN.

2. Switch #2 examines the PDU it receives on port 2 and notes that it does not have a VLAN with a VID 11. In response, it creates the VLAN as a dynamic GVRP VLAN, assigning it a VID 11 and the name GVRP_VLAN_11. (The name of a dynamic GVRP VLAN has the prefix "GVRP_VLAN_", followed by the VID number.) The switch then adds port 2, the port that received the PDU, as a tagged member of the VLAN.

3. Switch #2 sends a PDU from port 3 containing all the VIDs of the VLANs on the switch, including the new GVRP_VLAN_11 with its VID of 11. (Note that port 3 is not yet a member of the VLAN. Ports are added to VLANs when they receive PDUs from other network devices, not when they transmit PDUs.)

4. Switch #3 receives the PDU on port 4 and, after examining it, notes that one of the VLANs on switch #2 has the VID 11, which matches the VID of an already existing VLAN on the switch. So it does not create the VLAN because it already exists. It then determines whether the port that received the PDU, in this case port 4, is a member of the VLAN. If it is not a member, it automatically adds the port to the VLAN as an tagged dynamic GVRP port. If the port is already a member of the VLAN, then no change is made.

5. Switch #3 sends a PDU out port 4 to switch #2.

6. Switch #2 receives the PDU on port 3 and then adds the port as a tagged dynamic GVRP port to the dynamic GVRP_VLAN_11 VLAN.

There is now a communications path for the end nodes of the Sales VLAN on switches #1 and #3. GVRP created the new GVRP_VLAN_11 dynamic GVRP VLAN with a VID of 11 on switch #2 and added ports 2 and 3 to the VLAN as tagged dynamic GVRP ports.

764

Guidelines

Here are the guidelines to GVRP:

❐ GVRP is supported with STP, RSTP, MSTP or without spanning tree.

❐ Both ports that constitute a network link between the switch and the other device must be running GVRP.

❐ You cannot modify or delete dynamic GVRP VLANs.

❐ You cannot remove dynamic GVRP ports from static or dynamic VLANs.

❐ To be detected by GVRP, a VLAN must have at least one active node or have at least one port with a valid link to an end node. GVRP cannot detect a VLAN that does not have any active nodes or valid port links.

❐ Resetting the switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The dynamic assignments are relearned by the switch as PDUs arrive on the ports from other switches.

❐ GVRP has three timers: Join Timer, Leave Timer, and Leave All Timer. The values for these timers must be set the same on all switches running GVRP. Timers with different values on different switches can result in GVRP compatibility problems.

❐ You can convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments.

❐ The default port settings on the switch for GVRP are active, meaning that the ports participate in GVRP. Allied Telesis recommends disabling GVRP on those ports that are connected to GVRP-inactive devices, meaning devices that do not feature GVRP.

❐ PDUs are transmitted from only those switch ports where GVRP is enabled.

GVRP and Network Security

GVRP should be used with caution because it can expose your network to unauthorized access. If a network intruder were to connect to a switch port running GVRP and transmit a bogus GVRP PDU containing VIDs of restricted VLANs, GVRP would make the port a member of the VLANs, giving the intruder access to restricted areas of your network.

Here are a couple of suggestions to protect against this type of network intrusion:

❐ Activating GVRP only on those switch ports connected to other GVRP devices. Do not activate GVRP on ports that are connected to GVRP-inactive devices.

❐ Converting all dynamic GVRP VLANs and dynamic GVRP ports to static assignments, and then turning off GVRP on all the switches. This preserves the new VLAN assignments while protecting against network intrusion.

GVRP-inactive Intermediate Switches

If two GVRP-active devices are separated by a GVRP-inactive switch, the GVRP-active devices may not be able to share VLAN information. There are two issues involved.

The first is whether the intermediate switch forwards the GVRP PDUs that it receives from the GVRP-active switches. GVRP PDUs are management frames, intended for the switch's CPU. In all likelihood, a GVRP-inactive switch will discard the PDUs because it will not recognize them.

The second issue is that even if a GVRP-inactive switch forwards GVRP PDUs, it will not create the VLANs, at least not automatically. Consequently, even if GVRP-active switches receive the PDUs and create the necessary VLANs, an intermediate switch may block the VLAN traffic, unless you modify its VLANs and port assignments manually.

Enabling GVRP on the Switch

The command for enabling GVRP on the switch is found in the Global Configuration mode. It is the GVRP ENABLE command. After the command is entered, the switch immediately begins to transmit PDUs from those ports where GVRP is enabled and to learn dynamic GVRP VLANs. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp enable
```

For reference information, refer to "GVRP ENABLE" on page 784.

Enabling GIP on the Switch

The *GARP Information Propagation* (GIP) component can be enabled separately from GVRP on the switch. GIP must be enabled if the switch is using GVRP. The command for activating GIP is the GVRP APPLICANT STATE ACTIVE command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp applicant state active
```

For reference information, refer to "GVRP APPLICANT STATE ACTIVE" on page 782.

Enabling GVRP on the Ports

To activate GVRP on the ports so that they transmit GVRP PDUs, use the GVRP REGISTRATION NORMAL command in the Port Interface mode. Because the default setting for GVRP on the ports is enabled, you should only need to use this command if you want to enable GVRP after disabling it on a port.

This example of the command activates GVRP on ports 12, 13 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12,port1.0.13,port1.0.17
awplus(config-if)# gvrp registration normal
```

For reference information, refer to "GVRP REGISTRATION" on page 785.

Setting the GVRP Timers

The switch has a Join Timer, a Leave Timer, and a Leave All Timer. You should not change the timers unless you understand their functions. (Refer to the IEEE 802.1p standard for the definitions.) The timers have to be set the same on all GARP-active network devices, and the Join Timer and Leave Timer have to be set according to the following equation:

Join Timer <= (2 x (Leave Timer))

The commands for setting the timers are in the Global Configuration mode. They are:

gvrp timer join *value*

gvrp timer leave *value*

gvrp timer leaveall *value*

The timers are set in one hundredths of a second. This example sets the Join Timer to 0.2 seconds, the Leave Timer to 0.8 seconds and the Leave All timer to 10 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer join 20
awplus(config)# gvrp timer leave 80
awplus(config)# gvrp timer leaveall 1000
```

For reference information, refer to "GVRP TIMER JOIN" on page 786, "GVRP TIMER LEAVE" on page 787 and "GVRP TIMER LEAVEALL" on page 788.

Disabling GVRP Timers on the Switch

To disable GVRP timer configurations, use the NO GVRP TIMER commands in the Global Configuration mode. They are:

`no gvrp timer join`

`no gvrp timer leave`

`no gvrp timer leaveall`

Use these commands to reset GVRP timers to the default values for each individual parameter. The default values are:

GVRP timer join: 20

GVRP timer leave: 60

GVRP timer leave all: 1000

For reference information, refer to "NO GVRP TIMER JOIN" on page 790, "NO GVRP TIMER LEAVE" on page 791 and "NO GVRP TIMER LEAVEALL" on page 792.

Disabling GVRP on the Ports

To disable GVRP on the ports, use the GVRP REGISTRATION NONE command in the Port Interface mode. This example of the command deactivates GVRP on ports 4 and 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4-1.0.5
awplus(config-if)# gvrp registration none
```

For reference information, refer to "GVRP REGISTRATION" on page 785.

Disabling GIP on the Switch

You can disable the GARP Information Propagation (GIP) component separately from GVRP on the switch. GIP must be enabled if the switch is using GVRP. There is never any reason to disable GIP. Even if the switch is not performing GVRP, you can still leave GIP enabled.

The command for disabling GIP is GVRP APPLICANT STATE NORMAL command. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp applicant state normal
```

For reference information, refer to "GVRP APPLICANT STATE NORMAL" on page 783.

774

Disabling GVRP on the Switch

To disable GVRP to stop the switch from learning any further dynamic VLANs or GVRP ports, use the NO GVRP ENABLE command in the Global Configuration mode. Here is the command.

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp enable
```

For reference information, refer to "NO GVRP ENABLE" on page 789.

Restoring the GVRP Default Settings

To disable GVRP and to return the timers to their default settings, use the PURGE GVRP command in the Global Configuration mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# purge gvrp
```

For reference information, refer to "PURGE GVRP" on page 793.

Displaying GVRP

Although there are five commands that display GVRP information, you will probably only need the SHOW GVRP TIMER command in the Privileged Exec mode. This command displays the status of GVRP and GIP on the switch and the three timer settings. Here is the command:

awplus# show gvrp timer

Here is an example of the information the command provides.

```
GVRP Status ............ Disabled
GVRP GIP Status ........ Disabled
GVRP Join Timer ........ 30
GVRP Leave Timer ....... 60
GVRP Leave All Timer ... 1000
```

Figure 138. SHOW GVRP TIMER Command

For reference information, refer to "SHOW GVRP APPLICANT" on page 794, "SHOW GVRP CONFIGURATION" on page 795, "SHOW GVRP MACHINE" on page 796, "SHOW GVRP STATISTICS" on page 797 and "SHOW GVRP TIMER" on page 799.

Chapter 50
GARP VLAN Registration Protocol Commands

The GARP VLAN registration protocol commands are summarized in Table 73 and described in detail within the chapter.

Table 73. GARP VLAN Registration Protocol Commands

Command	Mode	Description
"CONVERT DYNAMIC VLAN" on page 781	VLAN Configuration	Converts dynamic GVRP VLANs and port assignments to static.
"GVRP APPLICANT STATE ACTIVE" on page 782	Global Configuration	Enables GIP on the switch.
"GVRP APPLICANT STATE NORMAL" on page 783	Global Configuration	Disables GIP.
"GVRP ENABLE" on page 784	Global Configuration	Enables GVRP.
"GVRP REGISTRATION" on page 785	Port Interface	Set a port's GVRP status.
"GVRP TIMER JOIN" on page 786	Global Configuration	Sets the GARP Join Timer.
"GVRP TIMER LEAVE" on page 787	Global Configuration	Sets the GARP Leave Timer.
"GVRP TIMER LEAVEALL" on page 788	Global Configuration	Sets the GARP Leave All timer.
"NO GVRP ENABLE" on page 789	Global Configuration	Disables GVRP on the switch.
"NO GVRP TIMER JOIN" on page 790	Global Configuration	Disables the GARP Join Timer.
"NO GVRP TIMER LEAVE" on page 791	Global Configuration	Disables the GARP Leave Timer.
"NO GVRP TIMER LEAVEALL" on page 792	Global Configuration	Disables the GARP Leave All timer.
"PURGE GVRP" on page 793	Global Configuration	Disables GVRP on the switch and returns the timers to their default values.

Table 73. GARP VLAN Registration Protocol Commands (Continued)

Command	Mode	Description
"SHOW GVRP APPLICANT" on page 794	User Exec and Privileged Exec	Displays parameters for the GIP-connected ring for the GARP application:
"SHOW GVRP CONFIGURATION" on page 795	User Exec and Privileged Exec	Displays parameters for the internal database for the GARP application.
"SHOW GVRP MACHINE" on page 796	User Exec and Privileged Exec	Displays parameters for the GID state machines for the GARP application.
"SHOW GVRP STATISTICS" on page 797	User Exec and Privileged Exec	Displays GARP packet and message counters.
"SHOW GVRP TIMER" on page 799	User Exec and Privileged Exec	Displays the GARP time values.

CONVERT DYNAMIC VLAN

Syntax

```
convert dynamic vlan
```

Parameters

None

Mode

VLAN Configuration mode

Description

Use this command to convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments.

Example

This example converts dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# convert dynamic vlan
```

GVRP APPLICANT STATE ACTIVE

Syntax

```
gvrp applicant state active
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable GIP on the switch. GIP must be enabled for GVRP to operate properly.

Example

This example enables GIP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp applicant state active
```

GVRP APPLICANT STATE NORMAL

Syntax

```
gvrp applicant state normal
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable GIP on the switch.

> **Note**
> Do not disable GIP if the switch is running GVRP. GIP is required for proper GVRP operation.

Example

This example disables GIP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp applicant state normal
```

GVRP ENABLE

Syntax

```
gvrp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable GVRP on the switch.

Example

This example enables GVRP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp enable
```

GVRP REGISTRATION

Syntax

gvrp registration *normal*|*none*

Parameters

normal
   Enables GVRP on a port. This is the default setting.

none
   Disables GVRP on a port.

Mode

Port Interface mode

Description

Use this command to enable or disable GVRP on a port. A port where GVRP is enabled transmits GVRP PDUs. A port where GVRP is disabled does not send GVRP PDUs.

Examples

This example enables GVRP on ports 5 and 6:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5,port1.0.6
awplus(config-if)# gvrp registration normal
```

This example disables GVRP on port 20:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20
awplus(config-if)# gvrp registration none
```

785

GVRP TIMER JOIN

Syntax

```
gvrp timer join value
```

Parameters

value

Specifies the Join Timer in centiseconds, which are one hundredths of a second. The range is 20 to 60 centiseconds. The default is 20 centiseconds.

Mode

Global Configuration mode

Description

Use this command to set the GARP Join Timer. This timer must be set in relation to the GVRP Leave Timer according to the following equation:

Join Timer <= (2 x (GVRP Leave Timer))

> **Note**
> The setting for this timer must be the same on all GVRP-active network devices.

Example

This command sets the Join Timer to 0.3 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer join 30
```

GVRP TIMER LEAVE

Syntax

```
gvrp timer leave value
```

Parameters

value
    Specifies the Leave Timer in centiseconds, which are one
    hundredths of a second. The range is 30 to 180 centiseconds. The
    default is 60 centiseconds.

Mode

Global Configuration mode

Description

Use this command to set the GARP Leave Timer.

> **Note**
> The setting for this timer must be the same on all GVRP-active
> network devices.

Example

This command sets the Leave Timer to 0.8 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer leave 80
```

GVRP TIMER LEAVEALL

Syntax

```
gvrp timer leaveall value
```

Parameters

value

Specifies the Leave All Timer in centiseconds. The range is 500 to 3000 centiseconds. The default is 1000 centiseconds.

Mode

Global Configuration mode

Description

Use this command to set the GARP Leave All timer.

Note
The settings for this timer must be the same on all GVRP-active network devices.

Example

This command sets the Leave All timer to 10 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer leaveall 1000
```

788

NO GVRP ENABLE

Syntax

```
no gvrp enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable GVRP on the switch.

Example

This example disables GVRP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp enable
```

NO GVRP TIMER JOIN

Syntax

```
no gvrp timer join
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable GVRP Join Timer configurations and return the GVRP Join Timer to its default value. This timer must only be disabled in relation to the GVRP Leave Timer according to the following equation:

Join Timer <= (2 x (GVRP Leave Timer))

Note
The setting for this timer must be the same on all GVRP-active network devices.

Example

This command sets the Join Timer to 0.2 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp timer join
```

NO GVRP TIMER LEAVE

Syntax

```
no gvrp timer leave value
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the GARP Leave Timer and return the GVRP Leave Timer to its default value. This timer must only be disabled in relation to the GVRP Join Timer according to the following equation:

Join Timer <= (2 x (GVRP Leave Timer))

> **Note**
> The setting for this timer must be the same on all GVRP-active network devices.

Example

This command sets the Leave Timer to 0.6 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp timer leave
```

NO GVRP TIMER LEAVEALL

Syntax

```
no gvrp timer leaveall
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the GARP Leave All timer and return the GVRP Leave All timer to its default value.

Note
The settings for this timer must be the same on all GVRP-active network devices.

Example

This command sets the Leave All timer to 10 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp timer leaveall
```

PURGE GVRP

Syntax

```
purge gvrp
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable GVRP on the switch and to return the timers to their default values.

Example

This example disables GVRP on the switch and returns the timers to their default values:

```
awplus> enable
awplus# configure terminal
awplus(config)# purge gvrp
```

SHOW GVRP APPLICANT

Syntax

```
show gvrp applicant
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the following parameters for the GIP-connected ring for the GARP application:

- ❑ GARP Application
- ❑ GIP contact
- ❑ STP ID

Example

This example displays the GIP-connected ring parameters:

```
awplus# show gvrp applicant
```

SHOW GVRP CONFIGURATION

Syntax

```
show gvrp configuration
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the following parameters for the internal database for the GARP application. Each attribute is represented by a GID index within the GARP application.

- ❒ GARP Application
- ❒ GID Index
- ❒ Attribute
- ❒ Used

Example

The following example displays the values of the internal database parameters:

```
awplus# show gvrp configuration
```

SHOW GVRP MACHINE

Syntax

```
show gvrp machine
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the following parameters for the GID state machines for the GARP application. The output is shown on a per-GID index basis; each attribute is represented by a GID index within the GARP application.

- ❑ VLAN
- ❑ Port
- ❑ App
- ❑ Reg

Example

This example displays the GID state machine parameters:

```
awplus# show gvrp machine
```

SHOW GVRP STATISTICS

Syntax

```
show gvrp statistics
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the current values of the following GARP packet and message counters:

- ❑ GARP application
- ❑ Receive: Total GARP Packets
- ❑ Transmit: Total GARP Packets
- ❑ Receive: Invalid GARP Packets
- ❑ Receive Discarded: GARP Disabled
- ❑ Receive Discarded: Port Not Listening
- ❑ Transmit Discarded: Port Not Sending
- ❑ Receive Discarded: Invalid Port
- ❑ Receive Discarded: Invalid Protocol
- ❑ Receive Discarded: Invalid Format
- ❑ Receive Discarded: Database Full
- ❑ Receive GARP Messages: LeaveAll
- ❑ Transmit GARP Messages: LeaveAll
- ❑ Receive GARP Messages: JoinEmpty
- ❑ Transmit GARP Messages: JoinEmpty
- ❑ Receive GARP Messages: JoinIn
- ❑ Transmit GARP Messages: JoinIn
- ❑ Receive GARP Messages: LeaveEmpty
- ❑ Transmit GARP Messages: LeaveEmpty
- ❑ Receive GARP Messages: LeaveIn
- ❑ Transmit GARP Messages: LeaveIn

❐ Receive GARP Messages: Empty

❐ Transmit GARP Messages: Empty

❐ Receive GARP Messages: Bad Message

❐ Receive GARP Messages: Bad Attribute

Example

This example displays the values of GARP packet and message counters:

```
awplus# show gvrp statistics
```

798

SHOW GVRP TIMER

Syntax

```
show gvrp timer
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the current values for the following GARP application parameters:

- ❐ GARP application protocol
- ❐ GVRP status
- ❐ GVRP GIP status
- ❐ GVRP Join Time
- ❐ GVRP Leave Time
- ❐ GVRP Leaveall Time
- ❐ Port information
- ❐ Mode

Example

This example displays the values of the GARP application parameters:

```
awplus# show gvrp timer
```

Chapter 51

MAC Address-based VLANs

This chapter contains the following topics:

Overview

As explained in Chapter 47, "Port-based and Tagged VLANs" on page 717, VLANs are used to create independent LAN segments within a network and are typically employed to improve network performance or security. The AT-9000 Switch offers several different types of VLANs, including port-based, tagged, and private VLANs. Membership in these VLANs is determined either by the port VLAN identifiers (PVIDs) assigned to the ports on the switch or, in the case of tagged traffic, by the VLAN identifiers within the packets themselves.

This chapter describes VLANs that are based on the source MAC addresses of the end nodes that are connected to the switch. With MAC address-based VLANs, only those nodes whose source MAC addresses are entered as members of the VLANs can share and access the resources of the VLANs. This is in contrast to port-based and tagged VLANs where any node that has access to a switch port can join them as a member.

One of the principle advantages of this type of VLAN is that it simplifies the task of managing network users that roam. These are users whose work requires that they access the network from different points at different times. The challenge for a network administrator is providing these users with the same resources regardless of the points at which they access the network. If you employed port-based or tagged VLANs for roaming users, you might have to constantly reconfigure the VLANs, moving ports to and from different virtual LANs, so that the users always have access to the same network resources. But with MAC address-based VLANs, the switch can assign network users to the same VLANs and network resources regardless of the ports from which they access the network.

Egress Ports Implementing MAC address-based VLANs involves more than entering the MAC addresses of the end nodes of the VLAN members. You must also designate the egress ports on the switch for the packets from the nodes. The egress ports define the limits of flooding of packets when a port receives a unicast packet with an unknown destination address (that is, an address that has not been learned by the MAC address table). Without knowing the egress ports of a MAC address-based VLAN, the switch would be forced to flood the packets on all ports, possibly resulting in security violations in which end nodes receive packets from other nodes in different VLANs.

Table 74 on page 803 illustrates a simple example of the mapping of addresses to egress ports for a MAC address-based VLAN of six nodes. The example consists of four workstations, a printer, and a server. Workstation 1, for instance, is connected to port 1 on the switch and is mapped to egress ports 5 for the server and 6 for the printer.

Table 74. Mappings of MAC Addresses to Egress Ports Example

MAC address	End Node	Switch Egress Port
00:30:84:54:1A:45	Workstation 1 (Port 1)	5, 6
00:30:84:C3:5A:11	Workstation 2 (Port 2)	5, 6
00:30:84:22:67:17	Workstation 3 (Port 3)	5, 6
00:30:84:78:75:1C	Workstation 4 (Port 4)	5, 6
00:30:79:7A:11:10	Server (Port 5)	1-4
00:30:42:53:10:3A	Printer (Port 6)	1-4

Obviously, mapping source MAC addresses to egress ports can become cumbersome if you are dealing with a MAC address-based VLAN that encompasses many ports and nodes. Fortunately, the egress ports of a VLAN are considered as a community and, as such, need only be designated as an egress port of one address in the VLAN to be considered an egress port of all the addresses.

For instance, referring to the previous example, if workstation 1 sends a packet containing an unknown destination MAC address, the switch does not flood the packet to just ports 5 and 6, even though those are the designated egress ports for packets from workstation 1. Rather, it floods it out all egress ports assigned to all the MAC addresses of the VLAN, except, of course, the port where the packet was received. In the example, the switch would flood the packet out ports 2 through 6.

The community characteristic of egress ports in MAC address-based VLANs relieves you from having to map each address to its corresponding egress port. Instead, you only need to be sure that all the egress ports in a MAC address-based VLAN are assigned to at least one address.

It is also important to note that a MAC address must be assigned at least one egress port to be considered a member of a MAC address-based VLAN. VLAN membership of packets from a source MAC address not assigned any egress ports is determined by the PVID of the port where the packets are received.

Because egress ports are considered as a community within a VLAN, you can simplify the mappings by assigning all the egress ports to just one MAC address and assigning the rest of the addresses to just one port. This makes adding or deleting MAC addresses or egress ports easier. Here is how the example might look.

Table 75. Revised Example of Mappings of MAC Addresses to Egress Ports

MAC Address	End Node	Egress Port
00:30:84:54:1A:45	Workstation 1 (Port 1)	1-6
00:30:84:C3:5A:11	Workstation 2 (Port 2)	1
00:30:84:22:67:17	Workstation 3 (Port 3)	1
00:30:84:78:75:1C	Workstation 4 (Port 4)	1
00:30:79:7A:11:10	Server (Port 5)	1
00:30:42:53:10:3A	Printer (Port 6)	1

The switch can support more than one MAC-address VLAN at a time, and ports can be egress members of more than one VLAN. While this can prove useful in some situations, it can also result in VLAN leakage in which traffic of one VLAN crosses the boundary into other VLANs.

The problem arises in the case of unknown unicast traffic. If the switch receives a packet from a member of a MAC address-based VLAN with an unknown destination address, it floods the packet on all egress ports of the VLAN. If the VLAN contains a port that is also serving as an egress port of another VLAN, the node connected to the port receives the flooded packets, even if it does not belong to the same VLAN as the node that generated the packet.

Here is an example. Assume that port 4 on a switch has been designated an egress port of three MAC address-based VLANs. Any unknown unicast traffic that the switch receives that belongs to any of the VLANs will be flooded out port 4. This means that whatever device is connected to the port receives the flooded traffic form all three VLANs.

If security is a major concern for your network, you might not want to assign ports as egress ports to more than one VLAN at a time when planning your MAC address-based VLANs.

When a packet whose source MAC address is part of a MAC address-based VLAN arrives on a port, the switch performs one of the following actions:

❑ If the packet's destination MAC address is not in the MAC address table, the switch floods the packet out all egress ports of the VLAN, excluding the port where the packet was received.

❑ If the packet's destination MAC address is in the MAC address table, and if the port where the address was learned is one of the VLAN's egress ports, the switch forwards the packet to the port.

❐ If the packet's destination MAC address is in the MAC address table, but the port where the address was learned is not one of the VLAN's egress ports, the switch discards the packet.

VLANs that Span Switches

To create a MAC address-based VLAN that spans switches, you must replicate the MAC addresses of the VLAN nodes on all the switches where the VLAN exists. The same MAC address-based VLAN on different switches must have the same list of MAC addresses.

Figure 139 illustrates an example of a MAC address-based VLAN that spans two AT-9000 Switches. The VLAN consists of three nodes on each switch. Table 76 on page 806 lists the details of the VLAN on the switches. Note that each VLAN contains the complete set of MAC addresses of all VLAN nodes along with the appropriate egress ports on the switches.
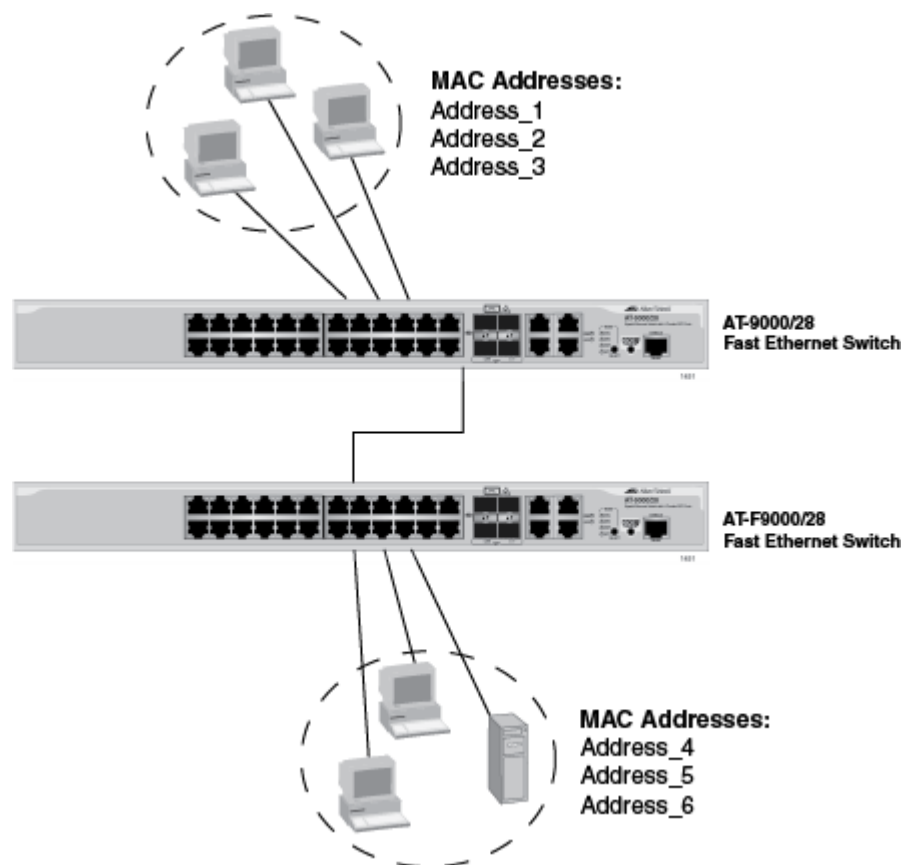
Figure 139. Example of a MAC Address-based VLAN that Spans Switches

Table 76. Example of a MAC Address-based VLAN Spanning Switches

Switch A		Switch B	
VLAN Name: Sales		VLAN Name: Sales	
MAC Address	Egress Ports	MAC Address	Egress Ports
Address_1	1,3,4,5	Address_1	11,12,14,16
Address_2	1	Address_2	11
Address_3	1	Address_3	11
Address_4	1	Address_4	11
Address_5	1	Address_5	11
Address_6	1	Address_6	11

VLAN Hierarchy

The switch employs a VLAN hierarchy when handling untagged packets that arrive on a port that is an egress port of a MAC address-based VLAN as well as an untagged port of a port-based VLAN. (A port can be a member of both types of VLANs at the same time.) The rule is that a MAC address-based VLAN takes precedence over that of a port-based VLAN.

When an untagged packet arrives on a port, the switch first compares the source MAC address of the packet against the MAC addresses of all the MAC address-based VLANs on the device. If there is a match, the switch considers the packet as a member of the corresponding MAC address-based VLAN and not the port-based VLAN, and forwards it out the egress ports defined for the corresponding MAC address-based VLAN.

If there is no match, the switch considers the packet as a member of the port-based VLAN and forwards the packet according to the PVID assigned to the port. For an explanation of a PVID, refer to "Port-based VLAN Overview" on page 720.

806

Guidelines

Here are the guidelines to MAC address-based VLANs:

❐ The switch can support up to a total of 4094 port-based, tagged, private, and MAC address-based VLANs.

❐ The egress ports of a MAC address-based VLAN function as a community in that assigning a port to one MAC address implicitly defines that port as an egress port of all the addresses in the same VLAN.

❐ A source MAC address must be assigned to at least one egress port to be considered part of a MAC address-based VLAN. Otherwise, VLAN membership is determined by the PVID of the port where the packets are received.

❐ A port can be an egress port of more than one MAC address-based VLAN at one time.

❐ MAC addresses can belong to only one MAC address-based VLAN at a time.

❐ Broadcast packets cross VLAN boundaries when a port is an egress port of a MAC address-based VLAN and an untagged member of a port-based VLAN. Given that there is no way for the switch to determine the VLAN to which the broadcast packet belongs, it floods the packet on all ports of all affected VLANs.

❐ Entering MAC addresses as part of a MAC address-based VLAN does not add them into the MAC address table. The addresses are added to the MAC address table during the normal learning process of the switch.

❐ MAC address-based VLANs are supported in edge switches, where end nodes are connected directly to the switches, as well as in intermediary switches, where the switches are connected to other Ethernet switches or hubs.

❐ The maximum number of MAC addresses that the switch can support in all its MAC address-based VLANs is 1024 addresses.

❐ MAC address-based VLANs do not support multicast MAC addresses.

❐ Egress ports cannot be part of static or LACP trunks.

❐ SFP ports 25 to 28 on the AT-9000/28SP Switch and SFP ports 49 to 52 on the AT-9000/52 Switch cannot be used as egress ports in MAC address-based VLANs.

General Steps

There are three main steps to creating a MAC address-based VLAN:

1. Use the VLAN MACADDRESS command in the VLAN Configuration mode to assign a name and a VID to the new VLAN, and to designate the VLAN as a MAC address-based VLAN.

2. Use the VLAN SET MACADDRESS command in the Global Configuration mode to assign the MAC addresses to the VLAN.

3. Use the VLAN SET MACADDRESS command in the Port Interface mode to assign the MAC addresses to the egress ports.

The steps must be performed in this order.

808

Creating MAC Address-based VLANs

The VLAN MACADDRESS command in the VLAN Configuration mode is the first command to creating this type of VLAN. This command assigns a new VLAN a name and a VID. Here is the format of the command:

```
vlan vid name name type macaddress
```

The range of the VID is 2 to 4094. The VID of the VLAN must be unique from all other VLANs on the switch. The name of a VLAN can be up to 20 characters. It cannot contain any spaces, and the first character must be a letter, not a number.

This example of the command creates a new MAC address-based VLAN with the VID 12 and the name QA:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 12 name QA type macaddress
```

For instructions on how to add MAC addresses and egress ports, refer to "Adding MAC Addresses to VLANs and Designating Egress Ports" on page 810.

Adding MAC Addresses to VLANs and Designating Egress Ports

The MAC addresses and egress ports are specified with the VLAN SET MACADDRESS command in the Global Configuration mode and Port Interface mode. Enter the command in the Global Configuration mode when you want to add MAC addresses to VLANs. To designate the egress ports of addresses, enter the same command in the Port Interface mode.

The command has the same format in both the Global Configuration mode and Port Interface mode. The format is shown here:

vlan set *vid macaddress|destaddress mac-address*

The VID parameter specifies the VID of the MAC address-based VLAN to which the address is to be added, and the MAC-ADDRESS parameter is the address, which has to be entered in this format:

xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

The MACADDRESS and DESTADDRESS keywords are equivalent. You can use either one in the command.

In this example of the command, the MAC address 2A:98:2C:AC:18:A4 is added to port 6 in a MAC address-based VLAN that has the VID 18:

awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# vlan set 18 macaddress 2a:98:2c:ad:18:a4	Use the VLAN SET MACADDRESS to add the MAC address to the VLAN.
awplus(config)# interface port1.0.6	Enter the Port Interface mode for port 6.
awplus(config-if)# vlan set 18 macaddress 2a:98:2c:ac:18:a4	Enter the VLAN SET MACADDRESS command again to designate port 6 as an egress port of the address.

810

Removing MAC Addresses

To remove MAC addresses from egress ports in a MAC address-based VLAN, use the NO VLAN MACADDRESS command in the Port Interface mode. This example of the command removes the MAC address 11:8A:92:CE:76:28 from ports 6 to 8, in a VLAN that has the VID 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6-port1.0.8
awplus(config-if)# no vlan 23 macaddress 11:8a:92:ce:76:28
```

Before MAC addresses can be completely removed from this type of VLAN, you must first remove them from their egress ports, as illustrated in the previous example. Afterwards, you can again use the NO VLAN MACADDRESS command, but in the Global Configuration mode, and delete them from the VLANs. This example completely removes the same MAC address from the same VLAN as in the previous example:

```
awplus> enable
awplus# configure terminal
awplus(config)# no vlan 23 macaddress 11:8a:92:ce:76:28
```

Deleting VLANs

To delete MAC address-based VLANs from the switch, use the NO VLAN command in the VLAN Configuration mode. You can delete only one VLAN at a time. Here is the format of the command:

```
no vlan vid
```

This example deletes the VLAN with the VID 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 23
```

Displaying VLANs

To display the MAC address-based VLANS on the switch, use the SHOW VLAN MACADDRESS command in the Privileged Exec mode:

```
awplus# show vlan macaddress
```

An example is shown in Figure 140.

```
VLAN 5 MAC Associations:
   Total number of associated MAC addresses: 5
   -------------------------------------------------
   MAC Address            Ports
   -------------------------------------------------
   5A:9E:84:31:23:85      port1.0.13-port1.0.18
   1A:87:9B:52:36:D5      port1.0.18
   26:72:9A:CB:1A:E4      port1.0.18
   89:01:BC:64:95:12      port1.0.18
   B2:89:10:02:1C:AE      port1.0.18
   -------------------------------------------------
VLAN 11 MAC Associations:
   Total number of associated MAC addresses: 5
   -------------------------------------------------
   MAC Address            Ports
   -------------------------------------------------
   78:3e:56:C8:AE:19      port1.0.8-port1.0.12
   AE:4B:76:18:54:C4      port1.0.12
   E7:98:03:12:C4:C5      port1.0.12
   7B:89:B2:AB:C4:57      port1.0.12
   89:EB:7B:34:82:CE      port1.0.12
   -------------------------------------------------
```

Figure 140. SHOW VLAN MACADDRESS Command

The fields are described in Table 78 on page 823.

Example of Creating a MAC Address-based VLAN

Here is an example of how to create this type of VLAN. This example creates the VLAN detailed in Table 75 on page 804. The example is named Sales and given the VID 21:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# vlan database`	Use the VLAN DATABASE command to enter the VLAN Configuration mode.
`awplus(config-vlan)# vlan 21 name Sales type macaddress`	Use the VLAN MACADDRESS to assign the name Sales and the VID 21 to the new VLAN, and to designate it as a MAC address-based VLAN.
`awplus(config-vlan)# exit`	Return to the Global Configuration mode.

`awplus(config)# vlan set 21 macaddress 00:30:84:54:1a:45`
`awplus(config)# vlan set 21 macaddress 00:30:84:c3:5a:11`
`awplus(config)# vlan set 21 macaddress 00:30:84:22:67:17`
`awplus(config)# vlan set 21 macaddress 00:30:84:78:75:1c`
`awplus(config)# vlan set 21 macaddress 00:30:79:7a:11:10`
`awplus(config)# vlan set 21 macaddress 00:30:42:53:10:3a`
	Use the VLAN SET MACADDRESS command in the Global Configuration mode to assign the MAC addresses to the VLAN.

`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show vlan macaddress`	Use the SHOW VLAN MACADDRESS command to confirm the MAC addresses.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.1`	Enter the Port Interface mode for port 1.

814

	Use the VLAN SET MACADDRESS command in the Port Interface mode to designate port 1 as an egress port of all the MAC addresses.

`awplus(config-if)# vlan set 21 macaddress 00:30:84:54:1a:45`
`awplus(config-if)# vlan set 21 macaddress 00:30:84:c3:5a:11`
`awplus(config-if)# vlan set 21 macaddress 00:30:84:22:67:17`
`awplus(config-if)# vlan set 21 macaddress 00:30:84:78:75:1c`
`awplus(config-if)# vlan set 21 macaddress 00:30:79:7a:11:10`
`awplus(config-if)# vlan set 21 macaddress 00:30:42:53:10:3a`	

`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan macaddress`	Confirm the configuration, again with the SHOW VLAN MACADDRESS command.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.2-port1.0.6`	Enter the Port Interface mode for ports 2 to 6.
`awplus(config-if)# vlan set 21 macaddress 00:30:84:54:1a:45`	Use the VLAN SET MACADDRESS command in the Port Interface mode to assign the ports one MAC address.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan macaddress`	Confirm the configuration with the SHOW VLAN MACADDRESS command.

815

Chapter 52

MAC Address-based VLAN Commands

The MAC address-based VLAN commands are summarized in Table 77 and described in detail within the chapter.

Table 77. MAC Address-based VLAN Commands

Command	Mode	Description
"NO VLAN" on page 818	VLAN Configuration	Deletes VLANs from the switch.
"NO VLAN MACADDRESS (Global Configuration Mode)" on page 819	Global Configuration	Removes MAC addresses from VLANs.
"NO VLAN MACADDRESS (Port Interface Mode)" on page 820	Port Interface	Removes MAC addresses from egress ports.
"SHOW VLAN MACADDRESS" on page 822	Privileged Exec	Displays MAC address-based VLANs.
"VLAN MACADDRESS" on page 824	VLAN Configuration	Assigns names and VIDs to new VLANs.
"VLAN SET MACADDRESS (Global Configuration Mode)" on page 826	Global Configuration	Adds MAC addresses to VLANs.
"VLAN SET MACADDRESS (Port Interface Mode)" on page 828	Port Interface	Adds MAC addresses to egress ports.

NO VLAN

Syntax

```
no vlan vid
```

Parameters

vid

> Specifies the VID of the VLAN you want to delete. You can specify just one VID.

Mode

VLAN Configuration mode

Description

Use this command to delete MAC address-based VLANs from the switch. You can delete only one VLAN at a time with this command.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 822

Example

This example deletes a MAC address-based VLAN with the VID 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 18
```

818

NO VLAN MACADDRESS (Global Configuration Mode)

Syntax

```
no vlan vid macaddress|destaddress mac-address
```

Parameters

vid
> Specifies the VID of the VLAN to be modified.

mac-address
> Specifies the MAC address to be removed from the VLAN. The MAC address must be entered in this format:
>
> xx:xx:xx:xx:xx:xx

Note
The MACADDRESS and DESTADDRESS keywords are equivalent.

Mode

Global Configuration mode

Description

Use this command to remove MAC addresses from MAC address-based VLANs. You can remove only one address at a time with this command. The command does not accept ranges or wildcards.

MAC addresses cannot be deleted if they are assigned to egress ports. To remove MAC addresses from egress ports, refer to "NO VLAN MACADDRESS (Port Interface Mode)" on page 820.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 822

Example

This example removes the MAC address 23:AC:2A:92:C1:53 from a MAC address-based VLAN with the VID 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# no vlan 11 macaddress 23:ac:2a:92:c1:53
```

819

NO VLAN MACADDRESS (Port Interface Mode)

Syntax

```
no vlan vid macaddress|destaddress mac-address
```

Parameters

vid

> Specifies the VID of the VLAN to be modified.

mac-address

> Specifies the MAC address to be removed from the VLAN. The MAC address must be entered in this format:
>
> xx:xx:xx:xx:xx:xx

> **Note**
> The MACADDRESS and DESTADDRESS keywords are equivalent.

Mode

Port Interface mode

Description

Use this command to remove MAC addresses from egress ports in MAC address-based VLANs.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 822

Examples

This example removes the MAC address 00:30:84:32:8A:5D from egress ports 1 and 4 in a VLAN that has the VID 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.4
awplus(config)# no vlan 17 macaddress 00:30:84:32:8a:5d
```

This example removes the MAC address 00:30:84:75:11:B2 from the egress port 11 to 14 in a VLAN with the VID 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.14
awplus(config)# no vlan 24 macaddress 00:30:84:75:11:b2
```

SHOW VLAN MACADDRESS

Syntax

```
show vlan macaddress
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the MAC addresses and the egress ports of the MAC address-based VLANs on the switch. An example is shown in Figure 141.

```
VLAN 11 MAC Associations:
   Total number of associated MAC addresses: 5
   -------------------------------------------------
   MAC Address            Ports
   -------------------------------------------------
   5A:9E:84:31:23:85      port1.0.4-port1.0.8
   1A:87:9B:52:36:D5      port1.0.4
   26:72:9A:CB:1A:E4      port1.0.4
   89:01:BC:64:95:12      port1.0.4
   B2:89:10:02:1C:AE      port1.0.4
   -------------------------------------------------
VLAN 12 MAC Associations:
   Total number of associated MAC addresses: 5
   -------------------------------------------------
   MAC Address            Ports
   -------------------------------------------------
   78:3e:56:C8:AE:19      port1.0.15-port1.0.22
   AE:4B:76:18:54:C4      port1.0.15
   E7:98:03:12:C4:C5      port1.0.15
   7B:89:B2:AB:C4:57      port1.0.15
   89:EB:7B:34:82:CE      port1.0.15
   -------------------------------------------------
```

Figure 141. SHOW VLAN MACADDRESS Command

822

The information is described here.

Table 78. SHOW VLAN MACADDRESS Command

Parameter	Description
VLAN *VID* MAC Associations	The VID of the MAC address-based VLAN.
Total Number of Associate MAC Addresses	Total number of MAC addresses that are assigned to the VLAN.
MAC Address	The MAC addresses of the VLAN.
Ports	The egress ports of the MAC addresses.

Example

The following example displays the MAC addresses and egress ports of the MAC address-based VLANs on the switch:

```
awplus# show vlan macaddress
```

VLAN MACADDRESS

Syntax

```
vlan vid name name type macaddress
```

Parameters

vid

Specifies a VLAN identifier in the range of 2 to 4094. VID 1 is reserved for the Default_VLAN. You can specify only one VID.

The VID of a VLAN should be unique from all other VLANs in a network, unless a VLAN spans multiple switches, in which case its VID should be the same on all switches on which the VLAN resides. For example, to create a VLAN called Sales that spans three switches, you would assign it the same VID value on each switch.

name

Specifies a name of up to 20 characters for the VLAN. The first character of the name must be a letter; it cannot be a number. VLANs will be easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). A name cannot be the same as a name of an existing VLAN on the switch. A VLAN that spans multiple switches should have the same name on each switch.

Mode

VLAN Configuration mode

Description

Use this command to create new MAC address-based VLANs. You can create just one VLAN at a time.

After creating a VLAN, use "VLAN SET MACADDRESS (Global Configuration Mode)" on page 826 to add MAC addresses to it and "VLAN SET MACADDRESS (Port Interface Mode)" on page 828 to assign the addresses to egress ports.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 822

Example

This example creates a MAC address-based VLAN that has the name Sales and the VID 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 3 name Sales type macaddress
```

VLAN SET MACADDRESS (Global Configuration Mode)

Syntax

```
vlan set vid macaddress|destaddress mac-address
```

Parameters

vid

      Specifies the VID of the VLAN to be modified.

mac-address

      Specifies the MAC address to be added to the VLAN. The MAC
      address must be entered in this format:

      xx:xx:xx:xx:xx:xx

Note
The MACADDRESS and DESTADDRESS keywords are equivalent.

Mode

Global Configuration mode

Description

Use this command to add MAC addresses to MAC address-based VLANs.
You can add only one address at a time with this command. You cannot
use ranges or wildcards.

The specified VLAN must already exist. Refer to "VLAN MACADDRESS"
on page 824 for instructions on how to create MAC address-based
VLANs. To add MAC addresses to egress ports, use "VLAN SET
MACADDRESS (Port Interface Mode)" on page 828.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 822

Examples

This example adds the MAC address 00:30:84:32:8A:5D to a MAC
address-based VLAN that has the VID 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan set 4 macaddress 00:30:84:32:8a:5d
```

This example adds the MAC address 00:30:84:32:76:1A to a MAC address-based VLAN with the VID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan set 12 macaddress 00:30:84:32:76:1a
```

VLAN SET MACADDRESS (Port Interface Mode)

Syntax

```
vlan set vid macaddress|destaddress mac-address
```

Parameters

vid
> Specifies the VID of the VLAN to be modified.

mac-address
> Specifies the MAC address to assign to an egress port. The MAC address must be entered in this format:
>
> xx:xx:xx:xx:xx:xx

Note
The MACADDRESS and DESTADDRESS keywords are equivalent.

Mode

Port Interface mode

Description

Use this command to assign MAC addresses to egress ports for MAC address-based VLANs. The specified MAC address must already be assigned to the VLAN. For instructions, refer to "VLAN SET MACADDRESS (Global Configuration Mode)" on page 826.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 822

Examples

This example assigns the MAC address 00:30:84:32:8A:5C to egress ports 1 and 4 in a VLAN whose VID is 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.4
awplus(config-if)# vlan set 3 macaddress 00:30:84:32:8a:5c
```

This example assigns the MAC address 00:30:84:75:11:B2 to ports 11 to 14 in a VLAN that has the VID 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.4
awplus(config-if)# vlan set 24 macaddress 00:30:84:75:11:b2
```

830

Chapter 53

Private Port VLANs

This chapter provides the following topics:

Overview

Private VLANs (also called private port VLANs) create special broadcast domains in which the traffic of the member ports is restricted to just uplink ports. Ports in a private VLAN are only allowed to forward traffic to and receive traffic from a designated uplink port, and are prohibited from forwarding traffic to each other.

An example application of a private VLAN would be a library in which user booths each have a computer with Internet access. In this situation, it would usually be undesirable to allow communication between these individual PCs. Connecting the computers to ports within a private isolated VLAN would enable each computer to access the Internet or a library server via a single connection, while preventing access between the computers in the booths.

Another application for private VLANs is to simplify IP address assignments. Ports can be isolated from each other while still belonging to the same subnet.

A private VLAN generally consists of one or more host ports and an uplink port.

Host Ports
The host ports of a private VLAN can only forward traffic to, and receive traffic from, an uplink port, and are prohibited from forwarding traffic to each other. A private VLAN can have any number of host ports on the switch, up to all the ports, minus the uplink port. A port can be a host port of only one private VLAN at a time.

The host ports are untagged. VLAN membership is defined by their PVIDs. The devices to which they are connected should not send tagged packets.

Uplink Port
The uplink port can be a promiscuous port or a trunk port.

An uplink port can communicate with all host ports in the private VLAN. A promiscuous port acts like an untagged uplink port for a private VLAN. Each private VLAN can have multiple promiscuous ports.

A trunk port may be configured as an uplink for a private VLAN.

832

Private VLAN Functionality

The following describes host and uplink port functionality in a private VLAN, and how private VLANs can be configured.

Host ports:

- ❒ Cannot communicate with each other.
- ❒ Can communicate with uplink ports.
- ❒ Can communicate with appropriately configured trunk ports.

Uplink ports:

- ❒ Promiscuous ports:

  – Promiscuous ports act as untagged trunk ports.

  – A private VLAN can have more than one promiscuous port.

- ❒ Trunk ports:

  – A private VLAN can be assigned to a trunk port as the native VLAN.

  – A private VLAN can be assigned to a trunk port as a tagged VLAN.

  – A trunk port that has been assigned a private VLAN can be assigned other VLANs.

Guidelines

Here are the guidelines to private VLANs:

❒ A private VLAN can have any number of host ports, up to all the ports on the switch, minus the uplink port.

❒ A promiscuous port can be an uplink port of just one private VLAN at a time, however, a private VLAN can have more than one uplink port.

❒ The host ports of private VLANs are untagged ports, and as such, transmit only untagged traffic.

❒ The switch can support private, port-based, tagged, and MAC address-based VLANs at the same time

❒ Host ports cannot be members of both private VLANs and port-based or tagged VLANs at the same time.

Creating Private VLANs

The command to initially create private VLANs is the PRIVATE-VLAN command in the VLAN Configuration mode. Here is the command's format:

```
private-vlan vid
```

The VID number has the range of 2 to 4094. The VID of a private VLAN must be unique from all other VLANs on the switch.

This example assigns the VID 26 to a new private VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 26
```

New private VLANs do not have any host or uplink ports. To add ports, refer to "Adding Host and Uplink Ports" on page 836.

Adding Host and Uplink Ports

Private VLANs have host ports and uplink ports. A private VLAN can have more than one uplink port. The devices connected to the hosts ports of a private VLAN can only communicate with the uplink port, and not with each other. The host ports and the uplink port can be added in any order to a private VLAN.

The SWITCHPORT MODE PRIVATE-VLAN HOST command in the Port Interface mode is used to add host ports to private VLANs. The command has this format:

```
switchport mode private-vlan host vid
```

The VID parameter is the VID of the private VLAN to which you are adding host ports. The private VLAN must already exist on the switch. Private VLANs are created with the PRIVATE-VLAN command, explained in "Creating Private VLANs" on page 835. This example of the command adds ports 2 to 7 as host ports of a private VLAN that has the VID 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.7
awplus(config-if)# switchport mode private-vlan host 15
```

The promiscuous uplink port of a private VLAN is designated with the SWITCHPORT MODE PRIVATE-VLAN PROMISCUOUS command in the Port Interface mode. Here is its format:

```
switchport mode private-vlan promiscuous vid
```

The VID parameter has the same function in this command as it does in the command for adding host ports. It designates the VLAN to which you want to add the port. This example of the command adds port 16 as an uplink port to a private VLAN that has the VID 23.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# switchport mode private-vlan promiscuous
23
```

> **Note**
> To add a private VLAN to a trunk port, either as a tagged VLAN or as the native VLAN, refer to "SWITCHPORT TRUNK ALLOWED VLAN" on page 753 or "SWITCHPORT TRUNK NATIVE VLAN" on page 756, respectively.

Deleting VLANs

To delete private VLANs from the switch, use the NO VLAN command in the VLAN Configuration mode. The host and uplink ports of deleted private VLANs are automatically returned by the switch to the Default_VLAN. Here is the format of the command:

```
no vlan vid
```

The VID parameter is the VID of the private VLAN you want to delete. The command lets you delete only one VLAN at a time. You cannot delete the Default_VLAN.

This example deletes a VLAN that has the VID 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 23
```

Displaying Private VLANs

The SHOW VLAN PRIVATE-VLAN command in the Privileged Exec mode displays the private VLANs currently existing on the switch, along with their host and uplink ports. Here is the command:

awplus# show vlan private-vlan

Here is an example of the display.

```
Private VLANs:
VID               Ports
-------------------------------------------------
12                4-8
28                17-24
```

Figure 142. SHOW VLAN PRIVATE-VLAN Command

Chapter 54

Private Port VLAN Commands

The private port VLAN commands are summarized in Table 79 and described in detail within the chapter.

Table 79. Private Port VLAN Commands

Command	Mode	Description
"NO VLAN" on page 840	VLAN Configuration	Deletes VLANs from the switch.
"PRIVATE-VLAN" on page 841	VLAN Configuration	Creates private port VLANs.
"SHOW VLAN PRIVATE-VLAN" on page 842	Privileged Exec	Displays the private port VLANs on the switch.
"SWITCHPORT MODE PRIVATE-VLAN HOST" on page 843	Port Interface	Adds host ports to private port VLANs.
"SWITCHPORT MODE PRIVATE-VLAN PROMISCUOUS" on page 844	Port Interface	Adds uplink ports to private port VLANs.

839

NO VLAN

Syntax

```
no vlan vid
```

Parameters

vid

Specifies the VID of the VLAN you want to delete. You can specify just one VID.

Mode

VLAN Configuration mode

Description

Use this command to delete private port VLANs from the switch. You can delete one VLAN at a time with this command.

Confirmation Command

"SHOW VLAN PRIVATE-VLAN" on page 842

Example

This example deletes a VLAN that has the VID 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 16
```

PRIVATE-VLAN

Syntax

```
private-vlan vid
```

Parameters

vid

> Specifies a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID must be unique from all VIDs of VLANs that currently exist on the switch. You can specify only one VID.

Mode

VLAN Configuration mode

Description

Use this command to create new private port VLANs. You can create just one VLAN at a time. Refer to "SWITCHPORT MODE PRIVATE-VLAN HOST" on page 843 to add host ports to a new VLAN, and to "SWITCHPORT MODE PRIVATE-VLAN PROMISCUOUS" on page 844 to designate an uplink port.

Confirmation Command

"SHOW VLAN PRIVATE-VLAN" on page 842

Example

This example creates a private port VLAN with the VID 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 23
```

SHOW VLAN PRIVATE-VLAN

Syntax

```
show vlan private-vlan
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the private-port VLANs on the switch. Here is an example of the information.

```
Private VLANs:
VID              Ports
-------------------------------------------------
12               4-8
28               17-24
```

Figure 143. SHOW VLAN PRIVATE-VLAN Command

Example

The following example displays the private-port VLANs on the switch:

```
awplus# show vlan private-vlan
```

SWITCHPORT MODE PRIVATE-VLAN HOST

Syntax

```
switchport mode private-vlan host vid
```

Parameters

vid

Specifies the VID of a private port VLAN to which ports are to be added as hosts. Specify a value between 1 and 4094.

Mode

Port Interface mode

Description

Use this command to add host ports to private port VLANs. Devices connected to host ports in a private port VLAN can only communicate with the uplink port.

Confirmation Command

"SHOW VLAN PRIVATE-VLAN" on page 842

Example

This example adds ports 15 to 18 as host ports of a private port VLAN with the VID 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15-port1.0.18
awplus(config-if)# switchport mode private-vlan host 23
```

SWITCHPORT MODE PRIVATE-VLAN PROMISCUOUS

Syntax

```
switchport mode private-vlan promiscuous vid
```

Parameters

vid

> Specifies the VID of a private port VLAN to which you are adding a promiscuous uplink port.

Mode

Port Interface mode

Description

Use this command to add a promiscuous uplink port to a private port VLAN. A promiscuous port can be an uplink port of just one private VLAN at a time.

Confirmation Command

"SHOW VLAN PRIVATE-VLAN" on page 842

Example

This example adds port 14 as an uplink port to a private port VLAN with the VID 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# switchport mode private-vlan promiscuous
15
```

Chapter 55
Voice VLAN Commands

The voice VLAN commands are summarized in Table 80 and described in detail within the chapter.

Table 80. Voice VLAN Commands

Command	Mode	Description
"NO SWITCHPORT VOICE VLAN" on page 846	Port Interface	Removes ports from voice VLANs.
"SWITCHPORT VOICE DSCP" on page 847	Port Interface	Configures the Layer 3 DSCP value advertised when LLDP-MED Network Policy TLVs are transmitted.
"SWITCHPORT VOICE VLAN" on page 848	Port Interface	Adds ports to voice VLANs.

NO SWITCHPORT VOICE VLAN

Syntax

```
no switchport voice vlan
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove a port from a voice VLAN. A port retains the CoS priority and DSCP values that were assigned to it when it was a voice VLAN member.

This command removes LLDP-MED network policy configuration for a voice device connected to these ports, but does not change the spanning-tree edge port status.

Confirmation Command

"SHOW VLAN" on page 746

Example

This example removes the voice VLAN assignment from port 1.0.24, and in turn, disables the transmission of LLDP-MED network policy information for voice devices on port 1.0.24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.24
awplus(config-if)# no switchport voice vlan
```

846

SWITCHPORT VOICE DSCP

Syntax

```
switchport voice dscp value
```

Parameters

value
   Specifies a DSCP value of 0 to 63.

Mode

Port Interface mode

Description

Use this command to assign a DSCP value to be advertised on a voice VLAN enabled port. A port transmits this value in its LLDP-MED network policy TLV to an IP phone, which, in turn, sends its packets using this DSCP value. A port can have both voice VLAN DSCP and CoS values.

Use the NO form of this command to remove a DSCP value from a port without replacing it with a new value. A DSCP value of 0 will be advertised.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example assigns the DSCP value 61 to ports 1.0.18 and 1.0.19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.19
awplus(config-if)# switchport voice dscp 61
```

This example removes the DSCP value from port 1.0.3, and a DSCP value of 0 will be advertised:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport voice dscp
```

SWITCHPORT VOICE VLAN

Syntax

```
switchport voice vlan <vid>|priority <value>
```

Parameters

vid

Specifies the ID number (VID) of the VLAN that functions as the voice VLAN for ports. You can specify only one VID. The range is 1 to 4094.

priority

Configures 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.

Mode

Port Interface mode

Description

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 form 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.

LLDP-MED advertisements, including Network Policy TLVs, are transmitted via a port if:

❒ LLDP is enabled (LLDP RUN command).

❒ The port is configured to transmit LLDP advertisements—enabled by default (LLDP TRANSMIT RECEIVE command).

❒ There is an LLDP-MED device connected to the port.

To set the priority value to be advertised for tagged frames, use the

848

SWITCHPORT VOICE VLAN PRIORITY command.

If the ports have been set to be edge ports by the SWITCHPORT VOICE VLAN command, the NO form of this command will leave them unchanged as edge ports. To set them back to their default non-edge port configuration, use the NO SPANNING-TREE PORTFAST command (refer to "NO SPANNING-TREE PORTFAST" on page 649).

The default setting for this feature is disabled.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

"SHOW LLDP LOCAL-INFO INTERFACE" on page 1125

Examples

This example tells IP phones connected to port 1.0.5 to send voice data tagged for VLAN 10:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice vlan 10
```

This example assigns the CoS value 5 to ports 1.0.2 and 1.0.3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.3
awplus(config-if)# switchport voice vlan priority 5
```

This example removes the CoS value from port 1.0.16 and returns to the default CoS value, 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# no switchport voice vlan priority
```

Chapter 56

VLAN Stacking

This chapter provides the following topics:

Overview

VLAN stacking is a way to label tagged and untagged packets with new 802.1Q headers. In the case of tagged packets, which already contain 802.1Q headers, VLAN stacking adds the new headers so that they coexist with the native headers in the packets.

This feature is intended for metro Ethernet providers. It allows them to uniquely label the individual packets of the customer traffic they transport over their networks, without having to delete any existing headers.

The headers consist of an EtherType value and a VLAN ID (VID). They are added as the customer packets enter the metro network networks and are removed when the packets reenter the customer networks. Thus, the packets reemerge unchanged on the customer networks, making the transition over the metro networks transparent to the customers.

VLAN stacking provides metro Ethernet providers with an alternative to using the native 802.1Q headers to identify and separate the private traffic flows that they transport across their public networks. In general, packets contain, at most, one 802.1Q header with one VID that identifies the VLAN, or broadcast domain, to which the node that generated a packet belongs. The drawback to using native headers is that different customers are likely to use the same VIDs in their networks. And requiring that customers reconfigure their VLANs by assigning unique VIDs not used by other customers is likely to be impractical.

VLAN stacking also provides a means for identifying packets that do not have 802.1Q headers, and therefore lack VIDs. VLAN memberships of packets without VIDs, referred to as untagged packets, are determined by the VIDs assigned to the ports on which the packets are received on the switches.

An 802.1Q header consists of two values. It has a VID and an EtherType/ Length value, which specifies either the protocol or the length of the data in the payload of a packet. VLAN stacking allows you to set both of these values.

The process of adding the extra 802.1Q header to packets is called encapsulation. It occurs at the point when packets leave a customer's network, prior to entering the metro Ethernet network. In the case of tagged packets, the extra 802.1Q header with the new EtherType/Length and VID values is added in front of the customer's 802.1Q header. The resulting packets have two VIDs, referred to as inner and outer VIDs. The outer VID belongs to the metro provider and the inner VID to the customer. A metro provider refers only to the outer VID when transporting packets across its network and ignores the inner VID. The outer VID resides in the packets only while the packets traverse their network and is removed

when they exit the network. The inner VID is native to the packets, but is ignored by the metro provider network.
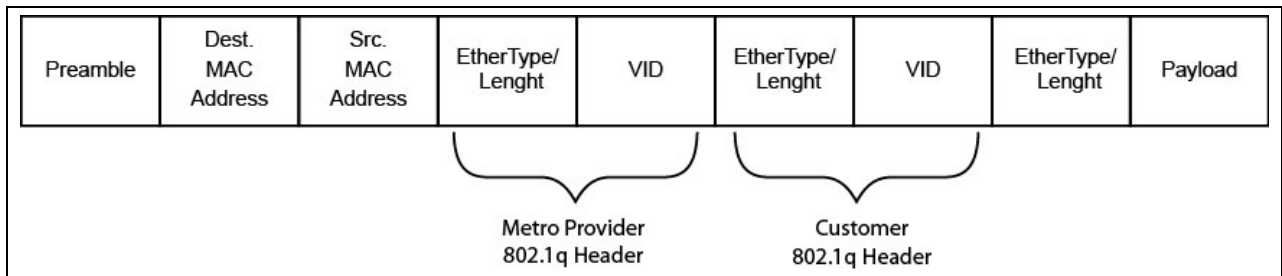
Figure 144. Metro Provider 802.1Q Header in Tagged Packets

VLAN stacking may also be used with untagged ports, which do not contain 802.1Q headers. The new header is added after the source MAC address and remains in the packets only while the packets are being transported across a metro network. The headers are deleted at the point the packets leave the metro network and reenter the customer networks.
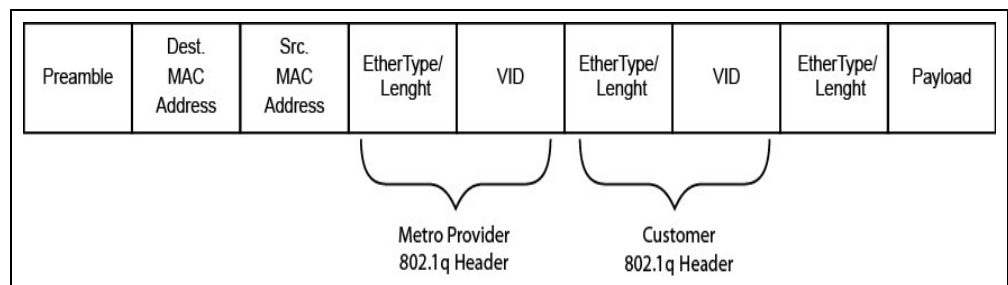
Figure 145. Metro Provider 802.1Q Header in Untagged Packets

Note
To maintain the best performance of a network in a metro environment and to avoid packet flooding on the ports on the switch, you should try to limit the number of network nodes to less than 8,000 devices, which is the maximum size of the switch's MAC address table.

Components

There are four components to VLAN stacking:

❒ VLAN

❒ Customer ports

❒ Provider port

❒ EtherType/Length value

VLAN

The boundary between the customer's network and the metro provider's network is marked by a VLAN. In cases where the switch is connected to more than one customer, there has to be a different VLAN for each customer.

The VID the VLAN is assigned has to be the VID that the metro provider wants to assign to the 802.1Q header that identifies the customer packets of that VLAN. For example, if a metro provider wants to assign the VID 110 to packets belonging to customer A, they would assign the VLAN the VID 110.

Customer Ports

Switch ports connected to devices on the customer's network are designated as customer ports. There can be more than one customer port in a VLAN.

Customer ports must be designated as untagged ports, meaning that they have to be in the VLAN access mode. Typically, untagged ports do not handle tagged packets. But with VLAN stacking, customer ports may handle tagged or untagged packets.

The extra 802.1Q headers are added to or deleted from the packets at the customer ports. The action of the ports depends on the direction of the packets. The new 802.1Q header is added to ingress tagged or untagged packets, prior to the packets being forwarded to the service provider port. The header is removed from egress packets, which are packets that customer ports are about to transmit to the customer's network. The headers are removed to return the packets to the same form that they had prior to entering the service provider network.

Provider Ports

Provider ports are switch ports that are connected to devices on the metro provider network. These ports have to be set to the tagged, trunk mode so that they do not delete the 802.1Q headers the customer ports add to the packets.

EtherType/ Length

This parameter specifies the protocol or length of the data in the payload in the packets. Also known as the Tag Protocol Identifier (TPID), this hexadecimal value has the range 0000 to FFFF. The EtherType/Length value is set at the switch level. The default value is 0x8100.

VLAN Stacking Process

Figure 146 illustrates the VLAN stacking process.
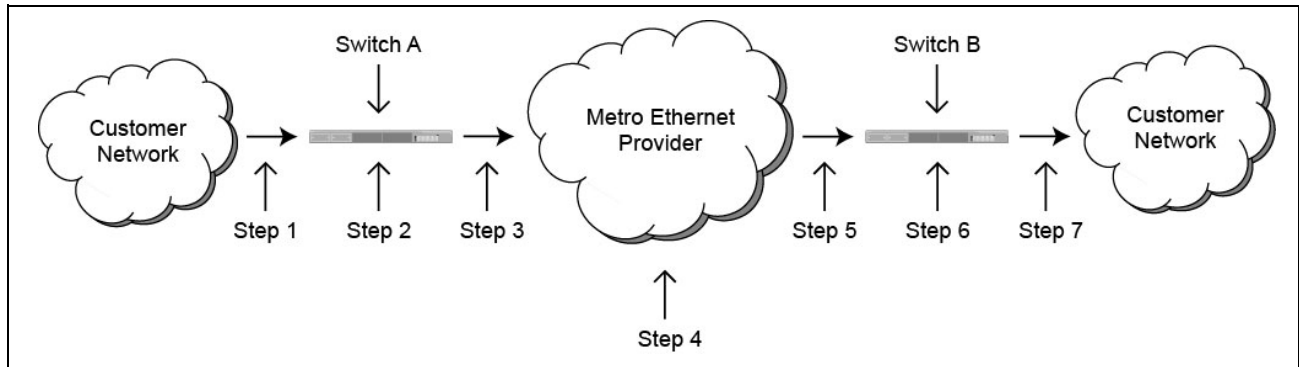
Figure 146. VLAN Stacking Process

The actions are described in Table 81.

Table 81. VLAN Stacking Process

Step	Action
1	A tagged or an untagged packet from the customer network is received by the customer port on switch A.
2	The customer port adds the new 802.1Q header, giving it the same VID number as the VLAN in which the customer port is a member.
3	The modified packet is forwarded out the provider port and into the metro Ethernet provider network.
4	The metro Ethernet provider network forwards the packet using the VID and EtherType/Length values in the new header added in step 2.
5	The packet arrives on the provider port on switch B.
6	The customer port deletes the header added in step 2, returning the packet to its original state.
7	The customer port transmits the packet to the customer network.

Example of VLAN Stacking

Here is an example of how to configure VLAN stacking. In the example, the customer's network is connected to ports 5 and 6 on the switch, and the provider's network is connected to port 7. Thus, ports 5 and 6 will be designated as customer ports and port 7 as the provider port. The service provider wants to use VID 79 to identify the packets of this customer. So the VID for the new VLAN has to be 79. The VLAN will be assigned the name ABC_Inc. This example also changes the EtherType/Length value to 0x8100.

The first step is to create the VLAN and assign it the VID 79:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# vlan database`	Enter the VLAN Configuration mode.
`awplus(config-vlan)# vlan 79 name ABC_Inc`	Create the new VLAN with the VLAN command.
`awplus(config-vlan)# end`	Return to the Global Configuration mode.
`awplus# show vlan`	Use the SHOW VLAN command to confirm the new VLAN.

```
VLAN ID   Name      Type      State     Member ports
                                        (u)-Untagged, (t) Tagged
=======   =======   =======   =======   ============================
1         default   STATIC    ACTIVE    port1.0.1(u)  port1.0.2(u)
                                        port1.0.3(u)  port1.0.4(u)
                                        port1.0.5(u)  port1.0.6(u)
                                        port1.0.7(u)  port1.0.8(u)
                                        port1.0.9(u)  port1.0.10(u)
                                        port1.0.11(u) port1.0.12(u)
                                        port1.0.13(u) port1.0.14(u)
                                        port1.0.15(u) port1.0.16(u)
                                        port1.0.17(u) port1.0.18(u)
                                        port1.0.19(u) port1.0.20(u)
                                        port1.0.21(u) port1.0.22(u)
                                        port1.0.23(u) port1.0.24(u)
                                        port1.0.25(u) port1.0.26(u)
                                        port1.0.27(u) port1.0.28(u)

79        ABC_Inc   STATIC    INACTIVE
```

The next steps add the customer ports to the VLAN.

awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface port1.0.5-port1.0.6	Enter the Port Interface mode for ports 5 and 6.
awplus(config-if)# switchport mode access	Use the SWITCHPORT MODE ACCESS command to designate the ports as untagged ports. As explained earlier, customer ports must be designated as untagged ports in VLAN stacking, even if the customer packets are tagged packets.
awplus(config-if)# switchport access vlan 79	Add the ports as untagged ports to the VLAN with the SWITCHPORT ACCESS VLAN command.
awplus(config-if)# switchport vlan-stacking customer-edge-port	Use the SWITCHPORT VLAN-STACKING command to designate the ports as customer ports.
awplus(config-if)# end	Return to the Global Configuration mode.
awplus# show vlan vlan-stacking	Use the SHOW VLAN VLAN-STACKING command to confirm the port configurations.

```
TPID       INTERFACES (c)-Customer-Edge Port, (p)-Provider Port
====       =========
0x8100     port1.0.5(c)
0x8100     port1.0.6(c)
```

This series of steps adds the provider port to the VLAN.

awplus# configure terminal	Enter the Global Configuration mode.
awplus(config-if)# interface port1.0.7	Move to the Port Interface mode for port 7.
awplus(config-if)# switchport mode trunk	Use the SWITCHPORT MODE TRUNK command to designate the port as a tagged port. The provider port must be designated as a tagged port.

`awplus(config-if)# switchport trunk allowed vlan add 79`	Add the port to the VLAN with the SWITCHPORT TRUNK ALLOWED VLAN command.
`awplus(config-if)# switchport vlan-stacking provider-port`	Use the SWITCHPORT VLAN-STACKING command to designate it as a provider port.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show vlan vlan-stacking`	Use the SHOW VLAN VLAN-STACKING command to confirm the port configurations.

```
TPID      INTERFACES (c)-Customer-Edge Port, (p)-Provider Port
====      =========
0x8100    port1.0.5(c)
0x8100    port1.0.6(c)
0x8100    port1.0.7(p)
```

`awplus# show vlan`	Use the SHOW VLAN command again to confirm the configuration of the ABC_Inc VLAN.

```
VLAN ID   Name      Type      State     Member ports
                                        (u)-Untagged, (t) Tagged
=======   =======   =======   =======   ============================
1         default   STATIC    ACTIVE    port1.0.1(u) port1.0.2(u)
                                        port1.0.3(u) port1.0.4(u)
                                        port1.0.7(u) port1.0.8(u)
                                        port1.0.9(u) port1.0.10(u)
                                        port1.0.11(u) port1.0.12(u)
                                        port1.0.13(u) port1.0.14(u)
                                        port1.0.15(u) port1.0.16(u)
                                        port1.0.17(u) port1.0.18(u)
                                        port1.0.19(u) port1.0.20(u)
                                        port1.0.21(u) port1.0.22(u)
                                        port1.0.23(u) port1.0.24(u)
                                        port1.0.25(u) port1.0.26(u)
                                        port1.0.27(u) port1.0.28(u)

79        ABC_Inc   STATIC    INACTIVE  port1.0.5(u) port1.0.6(u)
                                        port1.0.7(t)
```

The final series of steps changes the EtherType/Length value to 0x8100.

`awplus# configure terminal`	Enter the Global Configuration mode.

`awplus(config)# platform vlan-stacking-tpid 8100`	Change the EtherType/Length value to 0x8100 with the PLATFORM VLAN-STACKING-TPID command.
`awplus# exit`	Return to the Privileged Exec mode.
`awplus# show vlan vlan-stacking`	Use the SHOW VLAN VLAN-STACKING command to confirm the change to the EtherType/ Length (TPID) value.

```
TPID      INTERFACES (c)-Customer-Edge Port, (p)-Provider Port
====      =========
0x8100    port1.0.5(c)
0x8100    port1.0.6(c)
0x8100    port1.0.7(p)
```

Chapter 57
VLAN Stacking Commands

The VLAN stacking commands are summarized in Table 82.

Table 82. VLAN Stacking Commands

Command	Mode	Description
"NO SWITCHPORT VLAN-STACKING" on page 862	Port Interface	Removes ports from VLAN stacking.
"PLATFORM VLAN-STACKING-TPID" on page 863	Global Configuration	Specifies the Tag Protocol Identifier (TPID) value.
"SHOW VLAN VLAN-STACKING" on page 864	Privileged Exec	Displays the port assignments of VLAN stacking
"SWITCHPORT VLAN-STACKING" on page 865	Port Interface	Enables VLAN stacking on a port and designates it as a customer-edge-port or provider-port.

NO SWITCHPORT VLAN-STACKING

Syntax

```
no switchport vlan-stacking
```

Parameters

None.

Mode

Port Interface mode

Description

Use this command to remove ports from VLAN stacking.

Confirmation Command

"SHOW VLAN VLAN-STACKING" on page 864

Example

This example removes ports 3 to 16 and 21 from VLAN stacking:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3-port1.0.16,port1.0.21
awplus(config-if)# no switchport vlan-stacking
```

PLATFORM VLAN-STACKING-TPID

Syntax

```
platform vlan-stacking-tpid tpid
```

Parameters

tpid   Specifies the Tag Protocol Identifier (TPID) value that applies to all frames carrying double tagged VLANs. The range is 0x0 to 0xFFFF. The switch can have just one TPID value. The value must be entered in hexadecimal format.

Mode

Global Configuration mode

Description

Use this command to specify the Tag Protocol Identifier (TPID) value that applies to all frames that are carrying double tagged VLANs. All nested VLANs must use the same TPID value.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158 or "SHOW VLAN VLAN-STACKING" on page 864

Example

This example sets the TPID to 0x9000:

```
awplus> enable
awplus# configure terminal
awplus(config)# platform vlan-stacking-tpid 9000
```

SHOW VLAN VLAN-STACKING

Syntax

```
show vlan vlan-stacking
```

Parameters

None.

Mode

Port Interface mode

Description

Use this command to display the port assignments of VLAN stacking. Here is an example of the information.

```
TPID       INTERFACES (c)-Customer-Edge Port, (p)-Provider Port
====       =========
0x9000     port1.0.1(c)
0x9000     port1.0.2(c)
0x9000     port1.0.3(c)
0x9000     port1.0.4(c)
0x9000     port1.0.5(c)
0x9000     port1.0.6(c)
0x9000     port1.0.7(c)
0x9000     port1.0.23(p)
```

Figure 147. SHOW VLAN VLAN-STACKING Command

Example

```
awplus> enable
awplus# show vlan vlan-stacking
```

SWITCHPORT VLAN-STACKING

Syntax

```
switchport vlan-stacking customer-edge-port|provider-port
```

Parameters

None.

Mode

Port Interface mode

Description

Use this command to enable VLAN stacking on a port and designate it as a customer-edge-port or provider-port. This is sometimes referred to as VLAN double-tagging, nested VLANs, or QinQ.

Confirmation Command

"SHOW VLAN VLAN-STACKING" on page 864

Examples

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.3
awplus(config-if)# switchport vlan-stacking customer-edge-
port
```

This example configures port 17 as provider-port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# switchport vlan-stacking provider-port
```

Section VIII
Port Security

This section contains the following chapters:

868

Chapter 58

MAC Address-based Port Security

This chapter contains the following topics:

Overview

This feature lets you control access to the ports on the switch based on the source MAC addresses of the network devices. You specify the maximum number of source MAC addresses that ports can learn. Ports that learn their maximum number of addresses discard packets that have new, unknown addresses, preventing access to the switch by any further devices.

As an example, if you configure port 3 on the switch to learn no more than five source MAC addresses, the port learns up to five address and forwards the ingress packets of the devices that belong to those addresses. If the port receives ingress packets that have source MAC addresses other than the five it has already learned, it discards those packets to prevent the devices from passing traffic through the switch.

Static Versus Dynamic Addresses

The MAC addresses that the ports learn can be stored as either static or dynamic addresses in the MAC address table in the switch. Ports that store the addresses as static addresses never learn any new addresses after they have learned their maximum number. In contrast, ports that store the addresses as dynamic addresses can learn new addresses when addresses are timed out from the table by the switch. The addresses are aged out according to the aging time of the MAC address table.

> **Note**
> For background information on the aging time of the MAC address table, refer to "Overview" on page 344.

Intrusion Actions

The intrusion actions define what the switch does when ports that have learned their maximum number of MAC addresses receive packets that have unknown source MAC addresses. The possible settings are:

❒ Protect - Ports discard those frames that have unknown MAC addresses. No other action is taken. For example, if port 14 is configured to learn 18 addresses, it starts to discard packets with unknown source MAC addresses after learning 18 MAC addresses.

❒ Restrict - This is the same as the protect action, except that the switch sends SNMP traps when the ports discard frames. For example, if port 12 is configured to learn two addresses, the switch sends a trap every time the port, after learning two addresses, discards a packet that has an unknown MAC address.

❒ Shutdown - The switch disables the ports and sends SNMP traps. For example, if port 5 is configured to learn three MAC addresses, it is disabled by the switch to prevent it from forwarding any further traffic if it receives a packet with an unknown source MAC address,

after learning three addresses. The switch also sends an SNMP trap.

Guidelines

Here are the guidelines to MAC address-based port security:

❒ The filtering of a packet occurs on the ingress port, not on the egress port.

❒ You cannot use MAC address-based port security and 802.1x port-based access control on the same port. To configure a port as an Authenticator or Supplicant in 802.1x port-based access control, you must remove MAC address-based port security.

❒ This type of port security is supported on optional SFP modules.

❒ You can manually add static addresses to ports that are configured for this security. The manually added addresses are not counted against the maximum number of addresses the ports can learn.

Configuring Ports

There are three things you need to decide before you configure MAC address-based port security on the ports. They are:

❒ What is the maximum number of source MAC addresses the ports can learn?

❒ Should the source MAC addresses learned by the ports be stored as dynamic or static addresses in the MAC address table?

❒ Is the intrusion action protect, restrict, or shutdown?

See Table 83 for a list of the commands.

Table 83. MAC Address-based Port Security Commands and Descriptions

To	Use This Command	Range
Set the maximum number of source MAC addresses a port can learn.	SWITCHPORT PORT-SECURITY MAXIMUM *value*	0 to 255 addresses
Configure ports to save the source MAC addresses as dynamic addresses in the MAC address table.	SWITCHPORT PORT-SECURITY AGING	-
Configure ports to save the source MAC addresses as static addresses in the MAC address table.	NO SWITCHPORT PORT-SECURITY AGING	-
Set the intrusion action on the ports.	SWITCHPORT PORT-SECURITY VIOLATION PROTECT|RESTRICT| SHUTDOWN	-

These commands are found in the Port Interface mode and can be entered in any order when you configure the ports.

Here are a few examples on how to use the commands. In this first example, ports 4 and 5 are configured to learn up to 25 source MAC addresses each, and to store the addresses as static addresses in the MAC address table. The intrusion action is set to protect so that the ports discard packets with unknown MAC addresses after they have learned the maximum number of addresses, but the switch does not send SNMP traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.5
awplus(config-if)# switchport port-security maximum 25
awplus(config-if)# no switchport port-security aging
awplus(config-if)# switchport port-security violation
protect
```

This example configures port 16 to learn 45 MAC addresses. The addresses are stored as dynamic addresses in the table so that inactive addresses are deleted, permitting the port to learn new addresses. The intrusion action is set to restrict so that the switch sends SNMP traps if the port, after learning 45 source MAC addresses, discards packets with unknown source MAC addresses:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# switchport port-security maximum 45
awplus(config-if)# switchport port-security aging
awplus(config-if)# switchport port-security violation
restrict
```

This example configures ports 8 and 20 to learn up to five MAC addresses each. The addresses are stored as static addresses in the table, so that they are never aged out, even when the source nodes are inactive. The intrusion action is set to Shutdown, which disables the ports if they receive packets with unknown source packets after they learn five MAC addresses:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8,port1.0.20
awplus(config-if)# switchport port-security maximum 5
awplus(config-if)# no switchport port-security aging
awplus(config-if)# switchport port-security violation
shutdown
```

After configuring the ports, go to "Displaying Port Settings" on page 876 to confirm the settings before activating port security.

Enabling MAC Address-based Security on Ports

After you have configured a port for MAC address-based security, as explained in "Configuring Ports" on page 872, and confirmed the settings, as explained in "Displaying Port Settings" on page 876, you are ready to activate the feature on the ports. This is accomplished with the SWITCHPORT PORT-SECURITY command in the Port Interface mode. This example of the command activates port security on ports 16 to 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16-port1.0.24
awplus(config-if)# switchport port-security
```

To confirm the activation, return to "Displaying Port Settings" on page 876. The Security Enabled field in the SHOW PORT-SECURITY INTERFACE command should have a status of Yes.

874

Disabling MAC Address-based Security on Ports

To remove MAC address-based security from ports, use the NO SWITCHPORT PORT-SECURITY command in the Port Interface mode. This example of the command removes port security from port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no switchport port-security
```

Note
To activate ports that were disabled by the shutdown intrusion action, refer to "NO SHUTDOWN" on page 211.

Displaying Port Settings

There are two commands that display information about the MAC address-based port security on the ports on the switch. The one that you are likely to use the most often is the SHOW PORT-SECURITY INTERFACE command in the Privileged Exec mode. It displays all the possible information. Here is the format of the command:

```
show port-security interface port
```

This example displays the settings for port 2:

```
awplus# show port-security interface port1.0.2
```

An example is shown in Figure 148.

```
Port Security Configuration - Port1.0.2
-----------------------------------------------
Security Enabled          : YES
Port Status               : ENABLED
Violation Mode            : PROTECT
Aging                     : NO
Maximum MAC Addresses     : 0
Current Learned Addresses : 0
Lock Status               : UNLOCKED
Security Violation Count  : 0
```

Figure 148. SHOW PORT-SECURITY INTERFACE Command

The fields are defined in Table 85 on page 882.

If you are interested in viewing just the number of packets the ports have discarded because they had invalid source MAC addresses, you can use the SHOW PORT-SECURITY INTRUSTION INTERFACE command. Here is the format of the command:

```
show port-security intrusion interface port
```

This example displays the number of discarded packets on port 17:

```
awplus# show port-security intrusion interface port1.0.17
```

Figure 149 is an example of the information.

```
Port Security Intrusion List (Last 256 Intrusions)
----------------------------------------------------------
Interface: Port 1.0.17    -   2 intrusion(s) detected

0015.77b1.8510  eccd.6d48.4488
```

Figure 149. Example of SHOW PORT-SECURITY INTRUSION INTERFACE Command

Chapter 59

MAC Address-based Port Security Commands

The MAC address-based port security commands are summarized in Table 84 and described in detail within the chapter.

Table 84. MAC Address-based Port Security Commands

Command	Mode	Description
"NO SWITCHPORT PORT-SECURITY" on page 880	Port Interface	Removes MAC address-based security from ports.
"NO SWITCHPORT PORT-SECURITY AGING" on page 881	Port Interface	Configures ports to add the source MAC addresses as static MAC address in the MAC address table.
"SHOW PORT-SECURITY INTERFACE" on page 882	Privileged Exec	Displays the security mode settings of the ports
"SHOW PORT-SECURITY INTRUSION INTERFACE" on page 885	Privileged Exec	Displays the number of packets the ports have discarded.
"SWITCHPORT PORT-SECURITY" on page 887	Port Interface	Activates MAC address-based security on ports.
"SWITCHPORT PORT-SECURITY AGING" on page 888	Port Interface	Configures ports to add the source MAC addresses as dynamic MAC address in the MAC address table.
"SWITCHPORT PORT-SECURITY MAXIMUM" on page 889	Port Interface	Specifies the maximum number of dynamic MAC addresses that ports can learn.
"SWITCHPORT PORT-SECURITY VIOLATION" on page 890	Port Interface	Specifies the intrusion actions of the ports.

NO SWITCHPORT PORT-SECURITY

Syntax

```
no switchport port-security
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove MAC address-based security from the ports.

Note
To activate ports that were disabled by the shutdown intrusion action, refer to "NO SHUTDOWN" on page 211.

Confirmation Command

"SHOW PORT-SECURITY INTERFACE" on page 882

Example

This example removes MAC address-based security from port 14:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# no switchport port-security
```

NO SWITCHPORT PORT-SECURITY AGING

Syntax

```
no switchport port-security aging
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure ports to add source MAC addresses as static addresses in the MAC address table. Because static addresses are never deleted from the table, ports that learn their maximum numbers of source MAC addresses cannot learn new addresses, even when the source nodes of the learned addresses are inactive.

Confirmation Command

"SHOW PORT-SECURITY INTERFACE" on page 882

Example

This example configures ports 6 and 10 to store the source MAC addresses as static addresses in the MAC address table:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6,port1.0.10
awplus(config-if)# no switchport port-security aging
```

SHOW PORT-SECURITY INTERFACE

Syntax

show port-security interface *port*

Parameters

port

        Specifies the port whose security mode settings you want to view. You can display more than one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display the security settings of the ports on the switch. An example of the information is shown in Figure 150.

```
Port Security Configuration - Port1.0.15
------------------------------------------------
Security Enabled          : YES
Port Status               : ENABLED
Violation Mode            : PROTECT
Aging                     : NO
Maximum MAC Addresses     : 0
Current Learned Addresses : 0
Lock Status               : UNLOCKED
Security Violation Count  : 0
```

Figure 150. SHOW PORT-SECURITY INTERFACE Command

The fields are described in Table 85.

Table 85. SHOW PORT-SECURITY INTERFACE Command

Field	Description
Port	Port number.
Security Enabled	The current status of MAC address-based security on the port. The security is active if the status is Yes and inactive if the status is No. To activate or deactivate security on the port, refer to "SWITCHPORT PORT-SECURITY" on page 887 or "NO SWITCHPORT PORT-SECURITY" on page 880, respectively.

882

Table 85. SHOW PORT-SECURITY INTERFACE Command (Continued)

Field	Description
Port Status	The status of the port. The status can be Enabled or Disabled. A port that has a status of Enabled can forward network traffic. A port that has a Disabled status was shut down by the switch because it has an intrusion action of shutdown, and it received a packet with an unknown source MAC address after learning its maximum number of addresses. A port can also have a status of Disabled if it was manually disabled with the SHUTDOWN command. To reactivate a port with a Disabled status, use "NO SHUTDOWN" on page 211.
Violation Mode	The intrusion action of the port. The actions are: ❐ Protect - Protect intrusion action ❐ Restrict - Restrict intrusion action ❐ Shutdown - Shut down intrusion action
Aging	The status of MAC address aging on the port. If the aging status is No, the MAC addresses that are learned on the port are added as static MAC addresses to the MAC address table, so that they are retained even when the source nodes are inactive. If the aging status is Yes, the MAC addresses that are learned on the port are stored as dynamic MAC addresses and are deleted when the source nodes are inactive. To configure the port to save the source MAC addresses as static addresses, refer to "NO SWITCHPORT PORT-SECURITY AGING" on page 881. To configure the port to save the source MAC addresses as dynamic addresses, refer to "SWITCHPORT PORT-SECURITY AGING" on page 888.

Table 85. SHOW PORT-SECURITY INTERFACE Command (Continued)

Field	Description
Maximum MAC Addresses	The maximum number of dynamic MAC addresses the port is allowed to learn. To set this parameter, refer to "SWITCHPORT PORT-SECURITY MAXIMUM" on page 889.
Current Learned Addresses	The number of MAC addresses that have been learned on the port.
Lock Status	Whether or not the port has learned its maximum number of MAC addresses. The port will have a Locked status if it has learned its maximum number of MAC addresses, and an Unlocked status if it has not learned its maximum number of MAC addresses.
Security Violation Count	The number of ingress packets the port has discarded because they had unknown source MAC address. The port does not discard packets until after it has learned its maximum number of MAC addresses. This information is also available with "SHOW PORT-SECURITY INTRUSION INTERFACE" on page 885.

Example

This example displays the port security settings for ports 5 to 8:

```
awplus# show port-security interface port1.0.5-port1.0.8
```

SHOW PORT-SECURITY INTRUSION INTERFACE

Syntax

```
show port-security intrusion interface port
```

Parameter

port
    Specifies a port. You can specify more than one port at a time.
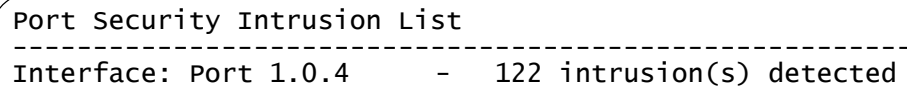
Modes

Privileged Exec mode

Description

Use this command to display the number of packets the ports have had to discard because the packets had unknown source MAC addresses. The ports begin to discard packets after learning their maximum number of source MAC addresses. This information is also available with "SHOW PORT-SECURITY INTERFACE" on page 882.

Figure 151 provides an example of the information.

```
Port Security Intrusion List
-----------------------------------------------------------
Interface: Port 1.0.4     -   122 intrusion(s) detected
```

Figure 151. SHOW PORT-SECURITY INTRUSION INTERFACE Command

Example

This command displays the number of discarded packets on port 15:

```
awplus# show port-security intrusion interface port1.0.15
```

Figure 152 on page 886 is an example of the information.

```
Port Security Intrusion List

Port Security Intrusion List (Last 10 Intrusions)
----------------------------------------------------------
Interface: Port 1.0.5     -   132 intrusion(s) detected

000:0900:127E 000:0900:127F 000:0900:027D
000:0900:027E 000:0900:027F 000:0900:1279
000:0900:127A 000:0900:127B 000:0900:127C
000:0900:127D
```

Figure 152. Example of SHOW PORT-SECURITY INTRUSION INTERFACE Command

SWITCHPORT PORT-SECURITY

Syntax

```
switchport port-security
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to activate MAC address-based security on ports.

Confirmation Command

"SHOW PORT-SECURITY INTERFACE" on page 882

Example

This example activates MAC address-based security on port 3 and ports 16 to 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3,port1.0.16-port1.0.18
awplus(config-if)# switchport port-security
```

SWITCHPORT PORT-SECURITY AGING

Syntax

```
switchport port-security aging
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure the ports to add the source MAC addresses as dynamic MAC address in the MAC address table. Ports that learn their maximum numbers of addresses can learn new addresses as inactive addresses are deleted from the table.

Confirmation Command

"SHOW PORT-SECURITY INTERFACE" on page 882

Example

This example sets port 2 to store its learned MAC addresses as dynamic addresses in the MAC address table:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security aging
```

SWITCHPORT PORT-SECURITY MAXIMUM

Syntax

```
switchport port-security maximum value
```

Parameters

value

Specifies the maximum number of dynamic MAC addresses ports can learn. The range is 0 to 255 addresses. The default is 0 addresses.

Mode

Port Interface mode

Description

Use this command to specify the maximum number of dynamic MAC addresses that ports can learn. Ports that learn their maximum numbers of MAC addresses discard ingress packets with unknown MAC addresses.

Use the no form of this command, NO SWITCHPORT PORT-SECURITY MAXIMUM, to set the command to its default value of 100 addresses.

Confirmation Command

"SHOW PORT-SECURITY INTERFACE" on page 882

Example

This example sets port 2 to learn up to 15 dynamic MAC addresses:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security maximum 15
```

SWITCHPORT PORT-SECURITY VIOLATION

Syntax

switchport port-security violation *protect*/*restrict*/
shutdown

Parameters

protect

Discards invalid frames. This is the default setting.

restrict

Discards invalid frames and sends SNMP traps.

shutdown

Sends SNMP traps and disables the ports.

Mode

Port Interface mode

Description

Use this command to specify the intrusion actions of the switch. The intrusion actions determine how the switch responds when ports that have learned their maximum number of MAC addresses receive ingress frames that have unknown source MAC addresses.

The no form of this command, NO SWITCHPORT PORT-SECURITY VIOLATION, returns the value to protect which is the default setting.

Confirmation Command

"SHOW PORT-SECURITY INTERFACE" on page 882

Examples

This example sets the intrusion action for port 5 to protect. The port, after learning its maximum number of MAC addresses, discards all ingress packets that have unknown MAC addresses:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport port-security violation
protect
```

This example sets the intrusion action for ports 22 to 24 to restrict. After learning their maximum numbers of MAC addresses, the ports discard packets with unknown source MAC addresses, and the switch sends SNMP traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22-port1.0.24
awplus(config-if)# switchport port-security violation
restrict
```

This example sets the intrusion action on port 2 to shutdown. The switch disables the port and sends an SNMP trap if the port learns its maximum number of MAC addresses and then receives an ingress packet with another unknown source MAC address:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security violation
shutdown
```

Chapter 60

802.1x Port-based Network Access Control

This chapter contains the following topics:

Overview

This chapter explains 802.1x port-based network access control. This port security feature lets you control who can send traffic through and receive traffic from the individual switch ports. The switch does not allow an end node to send or receive traffic through a port until the user of the node has been authenticated by a RADIUS server.

This feature is used to prevent unauthorized individuals from connecting a computer to a switch port or using an unattended workstation to access your network resources. Only those users designated as valid network users on a RADIUS server are permitted to use the switch to access the network.

This port security method uses the RADIUS authentication protocol. The management software of the switch includes RADIUS client software. If you have already read Chapter 88, "RADIUS and TACACS+ Clients" on page 1391, then you know that you can also use the RADIUS client software on the switch, along with a RADIUS server on your network, to create new remote manager accounts.

> **Note**
> RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication protocol for 802.1x port-based network access control. This feature is not supported with the TACACS+ authentication protocol.

Here are several terms to keep in mind when using this feature.

❒ Supplicant - A supplicant is an end user or end node that wants to access the network through a switch port. A supplicant may also be referred to as a client.

❒ Authenticator - The authenticator is a port that prohibits network access until a supplicant has logged on and been validated by the RADIUS server.

❒ Authentication server - The authentication server is the network device that has the RADIUS server software. This is the device that does the actual authenticating of the supplicants.

The switch does not authenticate any supplicants connected to its ports. Its function is to act as an intermediary between the supplicants and the authentication server during the authentication process.

Authentication Process

Below is a brief overview of the authentication process that occurs between a supplicant, authenticator, and authentication server. For further details, refer to the IEEE 802.1x standard.

❑ Either the authenticator (that is, a switch port) or the supplicant initiates an authentication message exchange. The switch initiates an exchange when it detects a change in the status of a port (such as when the port transitions from no link to valid link), or if it receives a packet on the port with a source MAC address not in the MAC address table.

❑ An authenticator starts the exchange by sending an EAP-Request/ Identity packet. A supplicant starts the exchange with an EAPOL-Start packet, to which the authenticator responds with an EAP-Request/Identity packet.

❑ The supplicant responds with an EAP-Response/Identity packet to the authentication server via the authenticator.

❑ The authentication server responds with an EAP-Request packet to the supplicant via the authenticator.

❑ The supplicant responds with an EAP-Response packet containing a username and password.

❑ The authentication server sends either an EAP-Success packet or EAP-Reject packet to the supplicant via the authenticator.

❑ Upon successful authorization of the supplicant by the authentication server, the switch adds the supplicant's MAC address to the MAC address as an authorized address and begins forwarding network traffic to and from the authorized supplicant.

❑ When the supplicant sends an EAPOL-Logoff message, the switch removes the supplicant's MAC address from the MAC address table, preventing the supplicant from sending or receiving any further traffic from the port.

Port Roles

Part of the task to implementing this feature is specifying the roles of the ports on the switch. The roles are listed here:

❑ None

❑ Authenticator

None Role
Switch ports in the none role do not participate in port-based access control. They forward traffic without authenticating the supplicants of the network devices. This is the default setting for the switch ports.

Note
A RADIUS authentication server cannot authenticate itself and must communicate with the switch through a port that is not configured as an authenticator port.

Authenticator Role
The authenticator role activates port access control on a port. Ports in this role do not forward network traffic to or from network devices until the supplicants are authenticated by a RADIUS server. The authenticator role is appropriate when you want the switch to authenticate the supplicants of network devices before they can use the network.

Note
There is also a supplicant role in 802.1x port-based network access control. However, the AT-9000 Series switches do not support that role. You can assign the ports to the none or authenticator role, but not the supplicant role.

896

Authentication Methods for Authenticator Ports

Authenticator ports support two authentication methods:

❒ 802.1x username and password combination

This authentication mode requires that the supplicants be assigned unique username and password combinations or digital certificates on the RADIUS server. A supplicant must provide the information either manually or automatically when initially passing traffic through an authenticator port and during reauthentications. The 802.1x client software on the supplicant either prompts the user for the necessary information or provides the information automatically.

Assigning unique username and password combinations to your network users and requiring the users to provide the information when they initially send traffic through the switch can enhance network security by limiting network access to only those supplicants who have been assigned valid combinations. Another advantage is that the authentication is not tied to any specific computer or node. An end user can log on from any system and still be verified by the RADIUS server as a valid user of the switch and network.

This authentication method requires 802.1x client software on the supplicant nodes.

❒ MAC address-based authentication

An alternative method is to use the source MAC format as the username and password combination for the device, for example: 00-00-01-00-00-00. The supplicant is not prompted for this information. Rather, the switch extracts the source MAC address from the initial frames received from a node and automatically sends it as both the username and password of the node to the RADIUS server for authentication.

The advantage to this approach is that the supplicant need not have 802.1x client software. The disadvantage is that because the supplicant is not prompted for a username and password combination, it does not guard against an unauthorized individual from gaining access to the network through an unattended network node or by counterfeiting a valid network MAC address.

Operational Settings for Authenticator Ports

An authenticator port can have one of three possible operational settings:

❒ Auto - Activates port-based authentication. The port begins in the unauthorized state, forwarding only EAPOL frames and discarding all other traffic. The authentication process begins when the link state of the port changes or the port receives an EAPOL-Start packet from a supplicant. The switch requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the RADIUS authentication server. After the supplicant is validated by the RADIUS server, the port begins forwarding all traffic to and from the supplicant.

❒ Force-authorized - Automatically places the port in the authorized state without any authentication exchange required. The port transmits and receives normal traffic without authenticating the supplicant.

❒ Force-unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The port forwards EAPOL frames, but discards all other traffic. This setting is analogous to disabling a port.

As mentioned earlier, the switch itself does not authenticate supplicants. That function is performed by the authentication server and the RADIUS server software. The switch acts as an intermediary for the authentication server by denying access to the network by the supplicant until the supplicant has been validated by the authentication server.

Operating Modes for Authenticator Ports

Authenticator ports have three modes:

❒ Single-host mode

❒ Multi-host mode

❒ Multi-supplicant mode

Single-Host Mode   An authenticator port set to the single-host mode permits only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant.

In Figure 153, port 1.0.6 is an authenticator port set to the single-host mode. It permits only one supplicant to log on and forwards the traffic of just that supplicant.

Port 1.0.6
Role: Authenticator
Operating Mode: Single-Host Mode

RADIUS Authentication Server

Authenticated Supplicant
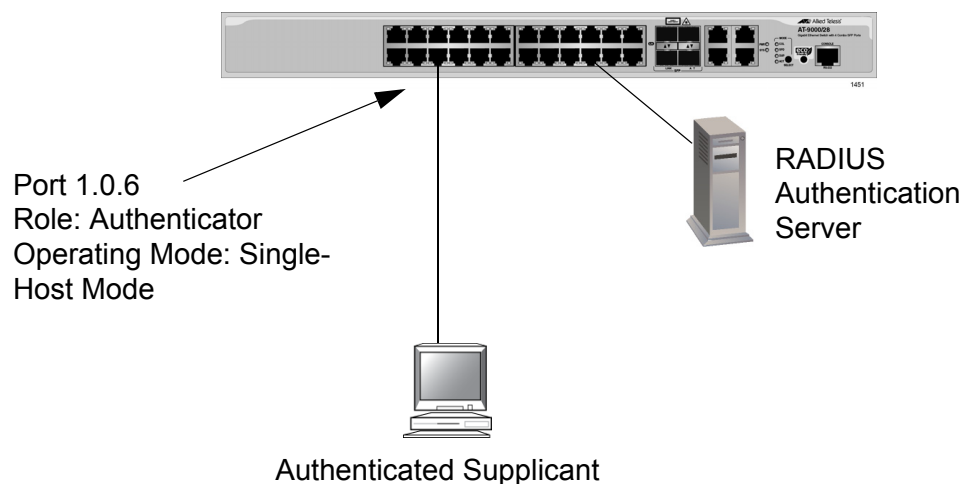
Figure 153. Single-Host Mode

Multi-Host Mode   This mode permits multiple supplicants on an authenticator port. An authenticator host forwards packets from all supplicants once one supplicant has successfully logged on. This mode is typically used in situations where you want to add 802.1x port-based network access control to a switch port that is supporting multiple supplicants, but do not want to create individual accounts for all the supplicants on the RADIUS server.

This is referred to as "piggy-backing." After one supplicant has successfully logged on, the port permits the other supplicants to piggy-back onto the initial supplicant's log on, so that they can forward packets through the port without being authenticated.

899

Note, however, that should the supplicant who performed the initial logon fail to periodically reauthenticate or log out, the authenticator port reverts to the unauthenticated state. It bars all further traffic to and from all the supplicants until the initial supplicant or another supplicant logs on.

Figure 154 is an example of this mode. Port 1.0.6 is connected to an Ethernet hub or non-802.1x compliant switch, which in turn is connected to several supplicants. The switch does not forward the supplicant traffic until one of the supplicants logs on. Afterwards, it forwards the traffic of all the supplicants.

Port 1.0.6
Role: Authenticator
Operating Mode: Multi-host mode

RADIUS
Authentication
server

Ethernet hub or
non-802.1x-
compliant
switch

Authenticated
Supplicant

Unauthenticated
Supplicants
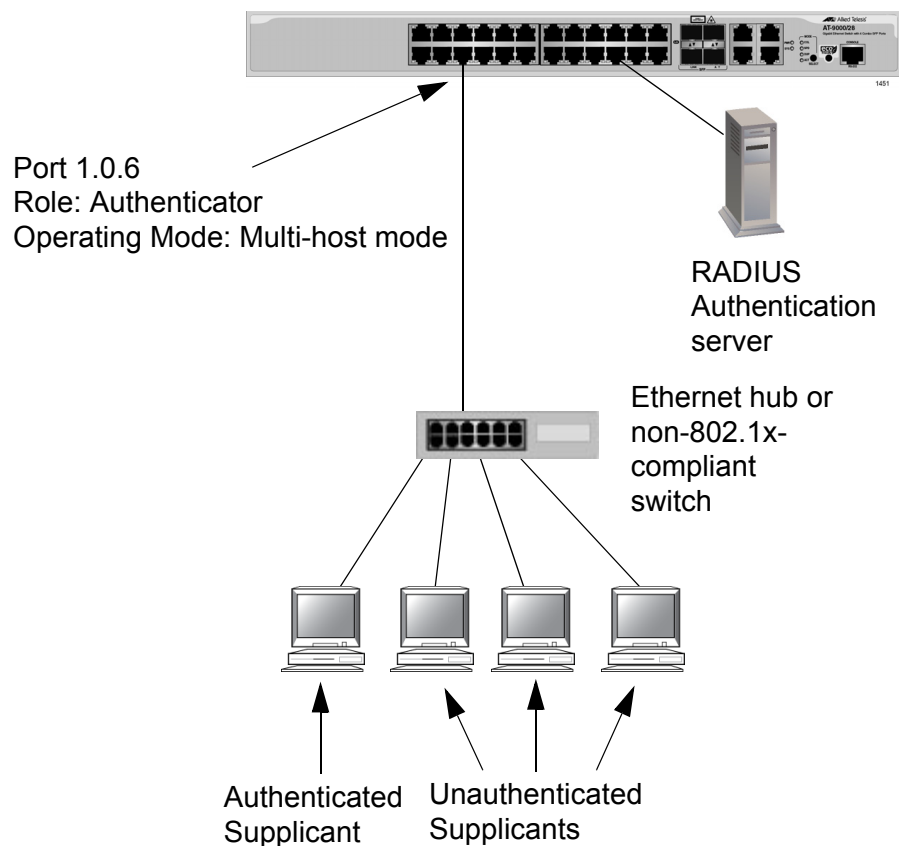
Figure 154. Multi-Host Operating Mode

If the port is configured as 802.1x Authenticator, one supplicant must have 802.1x client firmware and must provide a username and password during authentication. (The other supplicants do not need 802.1x client firmware to forward traffic through the port after one supplicant has been authenticated.)

If the port is using MAC address-based authentication, 802.1x client firmware is not required. The MAC address of the first supplicant to forward traffic through the port is used for authentication. When that supplicant is authenticated, all supplicants have access to the port.

As mentioned earlier, should the supplicant who performed the initial logon fail to reauthenticate when necessary or log out, the port reverts to the unauthenticated state, blocking all traffic to and from all supplicants. Another supplicant must be authenticated in order for all remaining supplicants to continue to forward traffic through the port.

Multi-Supplicant Mode

This mode authenticates all the supplicants on an authenticator port. This mode is appropriate in situations where an authenticator port is supporting more than one supplicant, and you want all supplicants to be authenticated. A switch can support up to a maximum of 208 supplicants.

If the authentication method is MAC address-based, the authenticator port uses the MAC addresses of the supplicants as the username and password combinations. The port accepts and forwards traffic only from those supplicants whose MAC addresses have been entered on the RADIUS server and denies access to all other users.

An example of this authenticator operating mode is illustrated in Figure 155 on page 902. The supplicants are connected to a hub or non-802.1x compliant switch which is connected to an authenticator port on the switch. If the port is configured as 802.1x Authenticator, the supplicants must successfully authenticate before they can forward traffic through the switch.

Port 1.0.6
Role: Authenticator
Operating Mode: Multi-Supplicant Mode

RADIUS
Authentication
Server

Ethernet Hub or
Non-802.1x-compliant
Switch

Authenticated
Supplicants
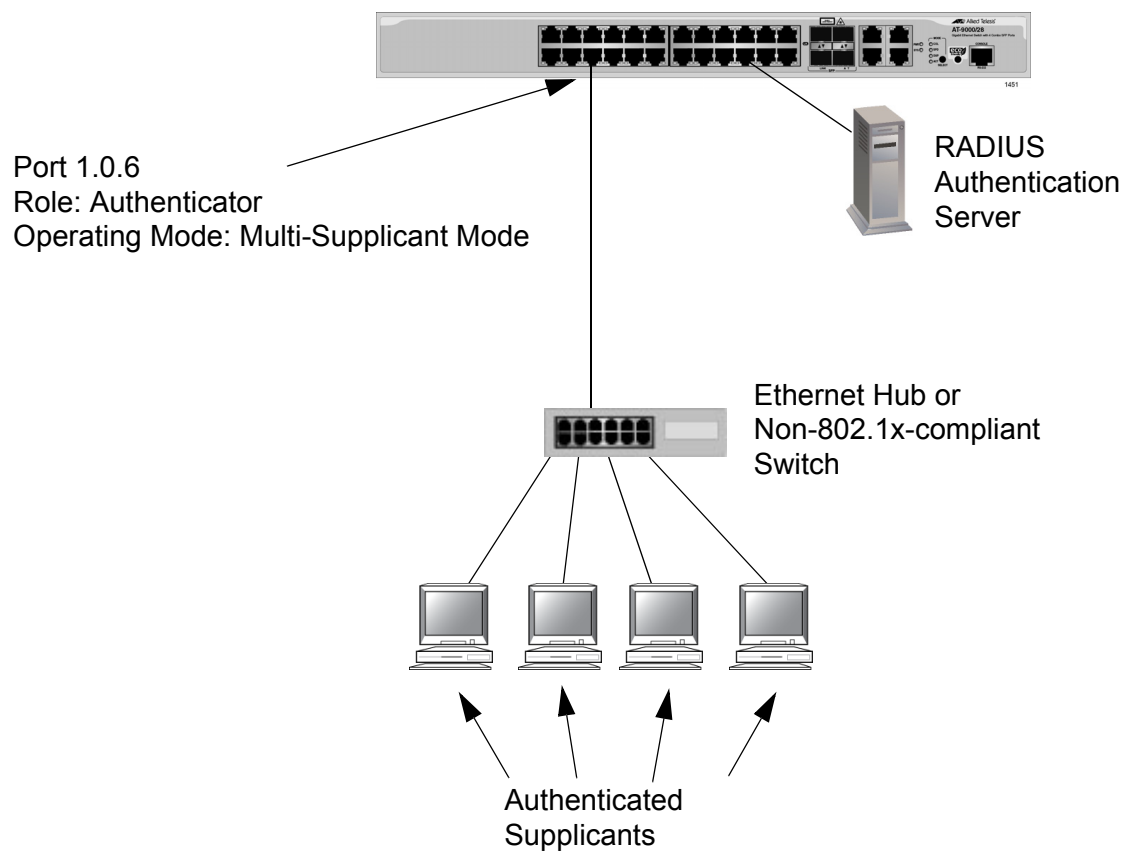
Figure 155. Multi-Supplicant Mode

Supplicant and VLAN Associations

One of the challenges to managing a network is accommodating end users who roam. These are individuals whose work requires that they access the network resources from different points at different times. The difficulty arises in providing them with access to the same network resources and, conversely, restricting them from unauthorized areas, regardless of the workstation from where they access the network. A closely related issue is where a workstation is employed at various times by different individuals with unique requirements in terms of network resources and security levels.

Providing network users with access to their network resources while also maintaining network security is often achieved through the use of VLANs. As explained in Chapter 47, "Port-based and Tagged VLANs" on page 717, a VLAN is an independent traffic domain where the traffic generated by the nodes within the VLAN is restricted to nodes of the same VLAN, unless there is a router or Layer 3 device. Different users are assigned to different VLANs depending on their resource requirements and security levels.

The problem with a port-based VLAN is that VLAN membership is determined by the port on the switch to which the device is connected. If a different device that needs to belong to a different VLAN is connected to the port, the port must be moved manually to the new VLAN using the management software.

With 802.1x port-based network access control, you can link a username and password combination or MAC address to a specific VLAN so that the switch automatically moves the port to the appropriate VLAN when a supplicant logs on. This frees the network manager from having to reconfigure VLANs as end users access the network from different points or where the same workstation is used by different individuals at different times.

To use this feature, you have to enter a VLAN identifier, along with other information, when you create a supplicant account on the RADIUS server. The server passes the identifier to the switch when a user logs on with a valid username and password combination or MAC address, depending on the authentication method. The information to provide on the RADIUS server is outlined in "Supplicant VLAN Attributes on the RADIUS Server" on page 905.

How the switch responds when it receives VLAN information during the authentication process can differ depending on the operating mode of the authenticator port.

Single-Host Mode

Here are the operating characteristics for the switch when an authenticator port is set to the single-host mode:

❐ If the switch receives a valid VLAN ID from the RADIUS server, it moves the authenticator port to the designated VLAN and changes the port to the authorized state. Only the authenticated supplicant is allowed to use the port. All other supplicants are denied entry.

❐ If the switch receives an invalid VLAN ID from the RADIUS server (for example, the VID of a nonexistent VLAN), it leaves the port in the unauthorized state to deny access to the port.

Multi-Host Mode

Here are the operating characteristics for the switch when an authenticator port is set to the multi-host mode:

❐ If the switch receives a valid VLAN ID from the RADIUS server, it moves the authenticator port to the designated VLAN and changes the port to the authorized state. All supplicants are allowed access to the port and the same VLAN after the initial authentication.

❐ If the switch receives an invalid VLAN ID from the RADIUS server (for example, the VID of a nonexistent VLAN), it leaves the port in the unauthorized state to deny access to the port.

Multi-Supplicant Mode

The initial authentication on an authenticator port running in the multi-supplicant mode is handled in the same fashion as with the single-host mode.

In multi-supplicant mode, how the switch handles subsequent authentications on the same port depends on whether dynamic VLAN creation is in one of the following states:

Disabled - NO AUTH DYNAMIC-VLAN-CREATION

If dynamic VLAN creation is disabled by issuing NO AUTH DYNAMIC-VLAN-CREATION, all supplicants that successfully authenticate will be made part of the VLAN of which the authenticator port is a member, regardless of the VLAN ID attribute in the RADIUS server response.

Enabled for single dynamic VLAN creation - AUTH DYNAMIC-VLAN-CREATION SINGLE

If dynamic VLAN creation is enabled by issuing AUTH DYNAMIC-VLAN-CREATION SINGLE, the first supplicant is authenticated and put in its VLAN per the RADIUS server response. Additional supplicants authenticating to the same VLAN as the first authenticated supplicant will be authenticated and placed in the VLAN. However, all other supplicants authenticating to a different VLAN will be denied access.

Enabled for multi dynamic VLAN creation - AUTH DYNAMIC-VLAN-CREATION MULTI

If dynamic VLAN creation is enabled by issuing AUTH DYNAMIC-VLAN-CREATION MULTI, each supplicant that successfully authenticates will be placed in its own VLAN.

Supplicant VLAN Attributes on the RADIUS Server

The following information must be entered as part of a supplicant's account on the RADIUS server when associating a supplicant to an untagged VLAN.

- ❐ Tunnel-Type
  The protocol to be used by the tunnel specified by Tunnel-Private-Group-Id. The only supported value is VLAN (13).

- ❐ Tunnel-Medium-Type
  The transport medium to be used for the tunnel specified by Tunnel-Private-Group-Id. The only supported value is 802 (6).

- ❐ Tunnel-Private-Group-ID
  The ID of the tunnel the authenticated user should use. This must be the name of VID of the VLAN of the switch.

The following information must be entered as part of a supplicant's account on the RADIUS server when associating a supplicant to a tagged VLAN:

Egress-VLANID attribute (specified in RFC4675 - used to specify 802.1Q tagged and untagged VLAN assignments with LLDP-MED/VoiceVLAN). The only supported value is Egress-VLANID (56).

For example: Egress-VLANID := 0x3100005A represents Tagged with VLANID = 90.

Note
Only "Tagged" is supported, that is the attribute value must begin with 0x31. For untagged VLANs, use Tunnel-Private-Group-ID.

Guest VLAN

An authenticator port in the unauthorized state typically accepts and transmits only 802.1x packets while waiting to authenticate a supplicant. However, you can configure an authenticator port to be a member of a guest VLAN when no supplicant is logged on or when a supplicant has failed authentication. Any supplicant using the port is not required to log on and has full access to the resources of the guest VLAN.

If the switch receives 802.1x packets on the port, signalling that a supplicant is logging on, the authentication process continues normally. If dynamic VLAN creation is enabled using AUTH DYNAMIC-VLAN-CREATION SINGLE, the authenticator port will be moved to the VLAN assigned by the RADIUS Server. If dynamic VLAN creation is disabled using NO AUTH DYNAMIC-VLAN-CREATION, after successful authentication, the port will be moved to Default VLAN 1, or the configured native VLAN (if a VLAN is configured). When the supplicant logs off, the port automatically returns to the guest VLAN.

Note
The Guest VLAN feature is only supported on an authenticator port in the Single-host operating mode.

Guidelines

Here are the general guidelines to this feature:

❑ Ports operating under port-based access control do not support dynamic MAC address learning.

❑ A port that is connected to a RADIUS authentication server must not be set to the authenticator role because an authentication server cannot authenticate itself.

❑ The authentication method of an authenticator port can be either 802.1x or MAC address-based, but not both.

❑ A supplicant connected to an authenticator port set to the 802.1x authentication method must have 802.1x client software.

❑ A supplicant does not need 802.1x client software if the authentication method of an authenticator port is MAC address-based.

❑ The maximum number of supported supplicants on the entire switch is 208.

❑ An 802.1x username and password combination is not tied to the MAC address of an end node. This allows end users to use the same username and password when working at different workstations.

❑ After a supplicant has successfully logged on, the MAC address of the end node is added to the switch's MAC address table as an authenticated address. It remains in the table until the supplicant logs off the network or fails to reauthenticate, at which point the address is removed. The address is not timed out, even if the node becomes inactive.

> **Note**
> End users of 802.1x port-based network access control should be instructed to always log off when they are finished with a work session. This can prevent unauthorized individuals from accessing the network through unattended network workstations.

❑ Authenticator ports cannot use MAC address-based port security. For further information, refer to Chapter 58, "MAC Address-based Port Security" on page 869.

❑ Authenticator ports cannot be members of static port trunks, LACP port trunks, or a port mirror.

❑ Authenticator ports cannot use GVRP.

❑ You cannot change the untagged VLAN assignment of a port after it has been designated as an authenticator port. To change the untagged VLAN assignment of an authenticator port, you must first

907

remove the authenticator designation. You can reapply the authenticator role to the port after moving it to its new VLAN assignment. Dynamic VLANs are supported only if the native VLAN is the default (that is, 1).

❐ To use the Guest VLAN feature, you have to manually create the VLAN. The switch does not create it automatically.

❐ The switch supports EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP authentication methods.

❐ The switch must have a management IP address to communicate with the RADIUS server. For background information, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

Here are the guidelines to adding VLAN assignments to supplicant accounts on a RADIUS server:

❐ The VLAN must be an 802.1q VLAN.

❐ The VLAN must already exist on the switch.

❐ A supplicant can have only one VLAN associated with it on the RADIUS server.

❐ When a supplicant logs on, the switch port is moved to an untagged/tagged VLAN as per the authenticator server's response.

Enabling 802.1x Port-Based Network Access Control on the Switch

To activate 802.1x Port-based Network Access Control on the switch, go to the Global Configuration mode and enter the AAA AUTHENTICATION DOT1X DEFAUT GROUP RADIUS command. The command has no parameters. Here is the command:

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

Note

You should configure the RADIUS client on the switch before activating port-based access control. For instructions, refer to Chapter 88, "RADIUS and TACACS+ Clients" on page 1391 or Chapter 89, "RADIUS and TACACS+ Client Commands" on page 1407.

Configuring Authenticator Ports

Designating Authenticator Ports

You have to designate ports as authenticator ports before you can configure their settings. There are three DOT1X PORT-CONTROL commands for designating authenticator ports.

The DOT1X PORT-CONTROL AUTO command designates ports such that they immediately begin to function as authenticator ports, blocking all traffic until supplicants successfully authenticate. This example of the command configures ports 1.0.1 and 1.0.5 to immediately commence functioning as authenticator ports.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.5
awplus(config-if)# dot1x port-control auto
```

> ⚠️ **Caution**
> Using the DOT1X PORT-CONTROL AUTO command when the switch is part of a live network interrupts network operations because the designated ports stop forwarding traffic until the supplicants log on.

Designating the Authentication Methods

A port can be configured for either 802.1x authentication or MAC based authentication.

To enable 802.1x authentication, use the DOTX PORT-CONTROL AUTO command. To configure a port to the MAC address authentication method, use the AUTH-MAC ENABLE command. This example configures port 1.0.16 as an authenticator port that uses the MAC address authentication method:

```
awplus> enable
awplus# configure terminal
awplus(config)# aaa authentication auth-mac default group radius
awplus(config)# radius-server host 176.225.15.23 key abt54
awplus(config)# interface port1.0.16
awplus(config-if)# auth-mac enable
```

If, after configuring an authenticator port for MAC address authentication, you decide to change it back to 802.1x authentication, use the NO AUTH-MAC ENABLE command and then use the DOTX PORT-CONTROL AUTO command. This example of the command restores 802.1x authentication to port 1.0.12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no auth-mac enable
awplus(config-if)# dotx port-control auto
```

Configuring the Operating Modes

As explained in "Operating Modes for Authenticator Ports" on page 899, authenticator ports have three operating modes:

❒ Single-host mode - For authenticator ports that are connected to a single node.

❒ Multi-host mode- For authenticator ports that are connected to multiple nodes. The ports forward all traffic after just one supplicant successfully logs on.

❒ Multi-supplicant mode - For authenticator ports that are connected to multiple nodes. The supplicants must log on individually before the ports forward their traffic.

The command for setting the operating mode is the AUTH HOST-MODE command in the Port Interface mode. The format of the command is shown here:

```
auth host-mode single-host| multi-host| multi-supplicant
```

This example configures port 1.0.1 as an authenticator port that uses the single-host mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# auth host-mode single-host
```

911

This example configures port 1.0.8 to use the multi-host mode so that it forwards traffic from all supplicants after just one supplicant logs on:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth host-mode multi-host
```

This example configures ports 1.0.16 to 1.0.19 to use the MAC address authentication method and the multi-supplicant mode so that the nodes are authenticated individually:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16-port1.0.19
awplus(config-if)# auth-mac enable
awplus(config-if)# auth host-mode multi-supplicant
```

912

Configuring Reauthentication

Table 86 lists the commands in the Port Interface mode for configuring reauthentication on authenticator ports. Reauthentication causes authenticator ports to periodically re-initiate authentication of supplicants. This is an additional security feature that protects your network by having supplicants periodically repeat the authentication process.

Table 86. Reauthentication Commands

To	Use This Command	Range
Activate reauthentication so that supplicants must periodically reauthenticate.	AUTH REAUTHENTICATION	-
Specify the time interval for reauthentication.	AUTH TIMEOUT REAUTH-PERIOD *value*	1 to 65,535 seconds
Remove reauthentication from ports.	NO AUTH REAUTHENTICATION	-

This example activates reauthentication on authenticator ports 1.0.21 and 1.0.22 so that the supplicants must reauthenticate every 2 hours (7200 seconds):

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21,port1.0.22
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth reauthentication
awplus(config-if)# auth timeout reauth-period 7200
```

This example deactivates reauthentication on port 1.0.21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# no auth reauthentication
```

Removing Ports from the Authenticator Role

To remove ports from the authenticator role so that they forward traffic without authenticating supplicants, go to the Port Interface mode of the ports and enter the NO DOT1X PORT-CONTROL command. This example removes the authenticator role from ports 1.0.1 to 1.0.4 and 1.0.18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4,port1.0.18
awplus(config-if)# no dot1x port-control
```

Disabling 802.1x Port-Based Network Access Control on the Switch

To disable 802.1x port-based network access control on the switch so that the ports forward packets without authentication, go to the Global Configuration mode and enter the NO AAA AUTHENTICATION DOT1X DEFAULT GROUP RADIUS command. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default group
radius
```

Note
The switch retains the configuration settings of the authenticator ports when 802.1x port-based network access control is deactivated. Authenticator ports will also not forward traffic of connected hosts until the dot1x interface configuration has also been negated.

Displaying Authenticator Ports

To view the settings of authenticator ports on the switch, use the SHOW DOT1X INTERFACE command in the Privileged Exec mode. This example displays the authenticator settings for port 1.0.2:

awplus# show dot1x interface port1.0.2

Figure 156 is an example of what you will see.

```
Authentication Info for interface port1.0.1
   portEnabled: Enabled - portControl: Auto
   portStatus: DOWN
   reAuthenticate: Disabled
   reAuthPeriod: 3600
   PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
   BE: suppTimeout: 30 - serverTimeout: 30
   CD: adminControlledDirections: in
   criticalVlan: Disabled
   guestVlan: Disabled
   dynamicVlanCreation: Multi-VLAN
   hostMode: Multi-Supplicant
   dot1x: Disabled
   protocolVersion: 1
   authMac: Disabled
   reAuthRelearning: Disabled
```

Figure 156. SHOW DOT1X INTERFACE Command

916

Displaying EAP Packet Statistics

To display EAP packet statistics of authenticator ports, use the SHOW DOT1X STATISTICS INTERFACE command. Here is an example of the information. This example displays the authenticator settings for port 1.0.2:

```
awplus> enable
awplus# show dot1x statistics interface port1.0.2
```

```
Authentication Statistics for interface port1.0.2
   EAPOL Frames Rx: 0 – EAPOL Frames Tx: 0
   EAPOL Start Frames Rx: 0 – EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 0 – EAP Response Frames Rx: 0
   EAP Req/Id Frames Tx: 0 – EAP Request Frames Tx: 0
   Invalid EAPOL Frames Rx: 0 – EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 0 – EAPOL Last Frame Src: 0000.0000.0000
```

Figure 157. SHOW DOT1X STATISTICS INTERFACE Command

918

Chapter 61

802.1x Port-based Network Access Control Commands

The 802.1x port-based network access control commands are summarized in Table 87 and described in detail within the chapter.

Table 87. 802.1x Port-based Network Access Control Commands

Command	Mode	Description
"AAA AUTHENTICATION DOT1X DEFAULT GROUP RADIUS" on page 922	Global Configuration	Activates 802.1x port-based network access control on the switch.
"AUTH DYNAMIC-VLAN-CREATION" on page 923	Port Interface	Configures the ports to accept dynamic VLAN allocation.
"AUTH GUEST-VLAN" on page 925	Port Interface	Enables and configures the Guest VLAN feature on an authenticator port.
"AUTH HOST-MODE" on page 926	Port Interface	Sets the operating modes on authenticator ports.
"AUTH REAUTHENTICATION" on page 928	Port Interface	Activates reauthentication on the authenticator ports.
"AUTH TIMEOUT QUIET-PERIOD" on page 929	Port Interface	Sets the number of seconds that authenticator ports wait after a failed authentication before accepting authentication requests again.
"AUTH TIMEOUT REAUTH-PERIOD" on page 930	Port Interface	Specifies the time interval for reauthentication of supplicants on an authenticator port.
"AUTH TIMEOUT SERVER-TIMEOUT" on page 931	Port Interface	Sets the length of time the switch waits for a response from the authentication server.
"AUTH TIMEOUT SUPP-TIMEOUT" on page 932	Port Interface	Sets the wait time in seconds for a response from a supplicant after a request has been sent.
"AUTH-MAC ENABLE" on page 933	Port Interface	Activates MAC address-based authentication on authenticator ports.

Table 87. 802.1x Port-based Network Access Control Commands (Continued)

Command	Mode	Description
"AUTH-MAC REAUTH-RELEARNING" on page 934	Port Interface	Sets the MAC address learning of the supplicant (client device) to relearning for re-authentication on the interface specified in the Interface command mode.
"DOT1X CONTROL-DIRECTION" on page 935	Port Interface	Sets the direction of the filter for the unauthorized interface.
"DOT1X EAP" on page 937	Global Configuration	Controls the action of the switch to EAP packets when 802.1x authentication is disabled on the switch.
"DOT1X INITIALIZE INTERFACE" on page 939	Port Interface	Forces authenticator ports into the unauthorized state and initializes authentication.
"DOT1X MAX-REAUTH-REQ" on page 940	Port Interface	Specifies the maximum number of times authenticator ports transmit EAP Request packets to supplicants before timing out authentication sessions.
"DOT1X PORT-CONTROL AUTO" on page 941	Port Interface	Sets ports to the authenticator role.
"DOT1X PORT-CONTROL FORCE-AUTHORIZED" on page 942	Port Interface	Configures ports to the 802.1x port-based authenticator role in the forced-authorized state.
"DOT1X PORT-CONTROL FORCE-UNAUTHORIZED" on page 943	Port Interface	Configures ports to the 802.1x port-based authenticator role in the forced-unauthorized state.
"DOT1X TIMEOUT TX-PERIOD" on page 944	Port Interface	Sets the amount of time the switch waits for a reply from a supplicant to an EAP-request/identity frame.
"NO AAA AUTHENTICATION DOT1X DEFAULT GROUP RADIUS" on page 945	Global Configuration	Disables 802.1x port-based network access control on the switch.
"NO AUTH DYNAMIC-VLAN-CREATION" on page 946	Port Interface	Disables dynamic VLAN assignments of authenticator ports.
"NO AUTH GUEST-VLAN" on page 947	Port Interface	Disables the Guest VLAN feature on an authenticator port.

Table 87. 802.1x Port-based Network Access Control Commands (Continued)

Command	Mode	Description
"NO AUTH REAUTHENTICATION" on page 948	Port Interface	Removes reauthentication from authenticator ports.
"NO AUTH-MAC ENABLE" on page 949	Port Interface	Deactivates MAC address-based authentication on authenticator ports.
"NO DOT1X PORT-CONTROL" on page 950	Port Interface	Removes ports from the authenticator role.
"SHOW AUTH-MAC INTERFACE" on page 951	Privileged Exec	Displays the parameter settings of authenticator ports.
"SHOW AUTH-MAC SESSIONSTATISTICS INTERFACE" on page 952	Privileged Exec	Displays the session status of the authenticator ports.
"SHOW AUTH-MAC STATISTICS INTERFACE" on page 953	Privileged Exec	Displays the authentication statistics of authenticator ports.
"SHOW AUTH-MAC SUPPLICANT INTERFACE" on page 954	Privileged Exec	Displays the supplicant state on authenticator ports.
"SHOW DOT1X" on page 955	Privileged Exec	Displays whether 802.1x port-based network access control is enabled or disabled on the switch and the IP address of the RADIUS server.
"SHOW DOT1X INTERFACE" on page 956	Privileged Exec	Displays the parameter settings of authenticator ports.
"SHOW DOT1X STATISTICS INTERFACE" on page 957	Privileged Exec	Displays EAP packet statistics on authenticator ports.
"SHOW DOT1X SUPPLICANT INTERFACE" on page 958	Privileged Exec	Displays the supplicant state on authenticator ports.

AAA AUTHENTICATION DOT1X DEFAULT GROUP RADIUS

Syntax

```
aaa authentication dot1x default group radius
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate 802.1x port-based network access control on the switch. The default setting for this feature is disabled.

Note
You should activate and configure the RADIUS client software on the switch before activating port-based access control. For instructions, refer to Chapter 88, "RADIUS and TACACS+ Clients" on page 1391 or Chapter 89, "RADIUS and TACACS+ Client Commands" on page 1407.

Confirmation Command

"SHOW DOT1X" on page 955

Example

This example activates 802.1x port-based network access control on the switch:

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

922

AUTH DYNAMIC-VLAN-CREATION

Syntax

```
auth dynamic-vlan-creation single| multi
```

Parameters

single

Single dynamic VLAN.

multi

Multiple dynamic VLAN.

Mode

Port Interface mode

Description

Use this command to dynamically assign a supplicant to a VLAN as instructed by the RADIUS Server.

Use the NO AUTH DYNAMIC-VLAN-CREATION to disable this feature (refer to "NO AUTH DYNAMIC-VLAN-CREATION" on page 946).

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Examples

This example activates single dynamic VLAN assignment on authenticator port 1.0.18. When the initial supplicant logs on, the switch moves the port to the VLAN specified in the supplicant's account on the RADIUS server.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation single
```

This example activates multiple dynamic VLAN assignment on authenticator port 1.0.4.

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation multiple
```

924

AUTH GUEST-VLAN

Syntax

```
auth guest-vlan vid
```

Parameters

vid

> Specifies the ID number of a VLAN that is the guest VLAN of an authenticator port. You can enter just one VID.

Mode

Port Interface mode

Description

Use this command to specify the VID of the VLAN that acts as the guest VLAN of an authenticator port. An authenticator port remains in a guest VLAN until a supplicant successfully logs on, at which point, it is moved to a configured VLAN; or if the dynamic VLAN setting is enabled, it will be moved to the VLAN specified in a supplicant's account on the RADIUS server.

A port must already be designated as an authenticator port before you can use this command.

To remove the VID of a guest VLAN from an authenticator port, refer to "NO AUTH GUEST-VLAN" on page 947.

Example

This example designates ports 1.0.1 to 1.0.4 as authenticator ports and specifies VID 12 as the guest VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth guest-vlan 12
```

AUTH HOST-MODE

Syntax

```
auth host-mode single-host| multi-host| multi-supplicant
```

Parameters

single-host
> Specifies the single-host operating mode. An authenticator port set to this mode forwards packets only from the one supplicant who initially logs on. This is the default setting.

multi-host
> Specifies the multi-host operating mode. An authenticator port set to this mode forwards all packets after one supplicant logs on. This is referred to as piggy-backing.

multi-supplicant
> Specifies the multi-supplicant operating mode. An authenticator port set to this mode requires that all supplicants log on.

Mode

Port Interface mode

Description

Use this command to set the operating modes on authenticator ports. For background information, refer to "Operating Modes for Authenticator Ports" on page 899.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Examples

This example configures authenticator ports 1.0.4 and 1.0.6 to the single-host operating mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.6
awplus(config-if)# auth host-mode single-host
```

This example configures authenticator port 1.0.8 to the multi-host operating mode, so that networks users can use the port after just one user logs on:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# auth host-mode multi-host
```

This example configures authenticator ports 1.0.12 and 1.0.13 to the multi-supplicant operating mode, which requires that all networks users on the ports log on:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12,port1.0.13
awplus(config-if)# auth host-mode multi-supplicant
```

AUTH REAUTHENTICATION

Syntax

```
auth reauthentication
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to activate reauthentication on the authenticator ports. The supplicants must periodically reauthenticate according to the time interval set with "AUTH TIMEOUT REAUTH-PERIOD" on page 930.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example activates reauthentication on ports 1.0.21 and 1.0.22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21,port1.0.22
awplus(config-if)# auth reauthentication
```

928

AUTH TIMEOUT QUIET-PERIOD

Syntax

```
auth timeout quiet-period value
```

Parameters

quiet-period

Sets the number of seconds that an authenticator port remains in the quiet state following a failed authentication exchange with a supplicant. The range is 1 to 65,535 seconds. The default value is 60 seconds.

Mode

Port Interface mode

Description

Use this command to set the number of seconds that an authenticator port waits after a failed authentication with a supplicant before accepting authentication requests again.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets the quiet period to 20 seconds on authenticator port 1.0.19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.19
awplus(config-if)# auth timeout quiet-period 20
```

AUTH TIMEOUT REAUTH-PERIOD

Syntax

```
auth timeout reauth-period value
```

Parameters

reauth-period

> Specifies the time interval that an authenticator port requires a supplicant to reauthenticate. The range is 1 to 65,535 seconds. The default value is 3600 seconds.

Mode

Port Interface mode

Description

Use this command to specify the time interval for reauthentication of supplicants on an authenticator port. Reauthentication must be enabled on an authenticator port for the timer to work. Reauthentication on a port is activated with "AUTH REAUTHENTICATION" on page 928.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example activates reauthentication on port 1.0.16 and sets the reauthentication interval to 12 hours:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# auth reauthentication
awplus(config-if)# auth timeout reauth-period 43200
```

930

AUTH TIMEOUT SERVER-TIMEOUT

Syntax

```
auth timeout server-timeout value
```

Parameters

server-timeout
> Sets the timer used by the switch to determine authentication server timeout conditions. The range is 1 to 65535 seconds. The default value is 30 seconds.

Mode

Port Interface mode

Description

Use this command to set the amount of time the switch waits for a response from a RADIUS authentication server.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets the timer on port 1.0.21 to 15 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# auth timeout server-timeout 15
```

AUTH TIMEOUT SUPP-TIMEOUT

Syntax

```
auth timeout supp-timeout value
```

Parameters

supp-timeout
> Sets the switch-to-supplicant retransmission time for EAP-request frames. The range is 1 to 65,535 seconds. The default value is 30 seconds.

Mode

Port Interface mode

Description

Use this command to set the retransmission time for EAP-request frames from authenticator ports.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets the retransmission time for EAP-request frames on authenticator ports 1.0.3 and 1.0.4 to 120 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3,port1.0.4
awplus(config-if)# auth timeout supp-timeout 120
```

932

AUTH-MAC ENABLE

Syntax

```
auth-mac enable
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to activate MAC address-based authentication on authenticator ports. An authenticator port that uses this type of authentication extracts the source MAC address from the initial frames from a supplicant and automatically sends it as the supplicant's username and password to the authentication server. This authentication method does not require 802.1x client software on supplicant nodes.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951

"SHOW DOT1X INTERFACE" on page 956

Example

This example activates MAC address-based authentication on ports 1.0.15 and 1.0.18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.18
awplus(config-if)# auth-mac enable
```

AUTH-MAC REAUTH-RELEARNING

Syntax

```
auth-mac reauth-relearning
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to set the MAC address of the supplicant (client device) to re-learning for re-authentication on the interface specified in the INTERFACE command.

Example

This example sets the MAC address of the supplicant to re-learning for re-authentication on port 1.0.23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# auth-mac reauth-relearning
```

934

DOT1X CONTROL-DIRECTION

Syntax

```
dot1x control-direction in|both
```

Parameters

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 value.

Mode

Port Interface mode

Description

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

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

If the **both** parameter is specified with this command, 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.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951

"SHOW DOT1X INTERFACE" on page 956

Examples

This example sets the port direction to the default (both) for port 1.0.2:

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

This example sets the port direction to **in** for port 1.0.2:

935

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

DOT1X EAP

Syntax

```
dot1x eap discard|forward|forward-untagged-vlan|
forward-vlan
```

Parameters

discard
Discards all ingress EAP packets on all ports.

forward
Forwards ingress EAP packets across all VLANs and ports.

forward-untagged-vlan
Forwards ingress EAP packets only to untagged ports in the same VLAN as the ingress port.

forward-vlan
Forwards ingress EAP packets to tagged and untagged ports in the same VLAN as the ingress port.

Mode

Global Configuration mode

Description

Use this command to control the action of the switch to EAP packets when 802.1x authentication is disabled on the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example configures the switch to forward all EAP packets when 802.1x authentication is disabled:

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

This example configures the switch to discard all EAP packets when 802.1x authentication is disabled:

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

This example configures the switch to forward EAP packets only to untagged ports in the VLANs of the ingress ports:

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

938

DOT1X INITIALIZE INTERFACE

Syntax

```
dot1x initialize interface port
```

Parameters

port
    Specifies a port. You can enter more than one port.

Mode

Privileged Exec mode

Description

Use this command to force authenticator ports into the unauthorized state. You might use this command to force supplicants on authenticator ports to reauthenticate themselves again by logging in with their usernames and passwords.

Example

This example forces authenticator ports 1.0.16 and 1.0.22 into the unauthorized state so that the supplicants must log on again:

```
awplus> enable
awplus# dot1x initialize interface port1.0.16,port1.0.22
```

DOT1X MAX-REAUTH-REQ

Syntax

```
dot1x max-reauth-req value
```

Parameters

max-reauth-req
> Specifies the maximum number of times the switch retransmits EAP Request packets to a supplicant before it times out an authentication session. The range is 1 to 10 retransmissions. The default value is 2.

Mode

Port Interface mode

Description

Use this command to specify the maximum number of times the switch transmits EAP Request packets to a supplicant before it times out the authentication session.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets the maximum number of requests on ports 1.0.7 and 1.0.22 to 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7,port1.0.22
awplus(config-if)# dot1x max-reauth-req 4
```

DOT1X PORT-CONTROL AUTO

Syntax

```
dot1x port-control auto
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to set the ports to the 802.1x port-based authenticator role. Ports begin in the unauthorized state, forwarding only EAPOL frames, until a supplicant has successfully logged on. For background information, refer to "Operational Settings for Authenticator Ports" on page 898.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets ports 1.0.7 to 1.0.10 to the authenticator role:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7-port1.0.10
awplus(config-if)# dot1x port-control auto
```

DOT1X PORT-CONTROL FORCE-AUTHORIZED

Syntax

```
dot1x port-control force-authorized
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure ports to the 802.1x authenticator role, in the force-authorized state. Ports that are set to the force-authorized state transition to the authorized state without any authentication exchanges required. The ports transmit and receive traffic normally without 802.1x based authentication of the supplicants. For background information, refer to "Operational Settings for Authenticator Ports" on page 898.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets ports 1.0.1 and 1.0.4 to the authenticator role, in the force-authorized state:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.4
awplus(config-if)# dot1x port-control force-authorized
```

DOT1X PORT-CONTROL FORCE-UNAUTHORIZED

Syntax

```
dot1x port-control force-unauthorized
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure the ports to the 802.1x authenticator role, in the unauthorized state. Although the ports are in the authenticator role, the switch blocks all traffic on the ports. For background information, refer to "Operational Settings for Authenticator Ports" on page 898.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets ports 1.0.7 and 1.0.24 to the authenticator role, in the force-unauthorized state:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7,port1.0.24
awplus(config-if)# dot1x port-control force-unauthorized
```

DOT1X TIMEOUT TX-PERIOD

Syntax

```
dot1x timeout tx-period value
```

Parameters

value

Sets the number of seconds an authenticator port waits for a response to an EAP-request/identity frame from a supplicant before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

Mode

Port Interface mode

Description

Use this command to set the amount of time that an authenticator port on the switch waits for a reply from a supplicant to an EAP-request/identity frame. If no reply is received, it retransmits the frame.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example sets the timeout period on authenticator ports 1.0.15 and 1.0.19 to 40 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.19
awplus(config-if)# dot1x timeout tx-period 40
```

944

NO AAA AUTHENTICATION DOT1X DEFAULT GROUP RADIUS

Syntax

no aaa authentication dot1x default group radius

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable 802.1x port-based network access control on the switch. All ports forward packets without any authentication. This is the default setting.

Confirmation Command

"SHOW DOT1X" on page 955

Example

This example disables 802.1x port-based network access control on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default group
radius
```

NO AUTH DYNAMIC-VLAN-CREATION

Syntax

```
no auth dynamic-vlan-creation
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable dynamic VLAN assignments of authentication ports. For background information, refer to "Supplicant and VLAN Associations" on page 903.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951

"SHOW DOT1X INTERFACE" on page 956

Example

This example disables dynamic VLAN assignment of authenticator port 1.0.15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# no auth dynamic-vlan-creation
```

NO AUTH GUEST-VLAN

Syntax

```
no auth guest-vlan
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the Guest VLAN feature on an authenticator port.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951

"SHOW DOT1X INTERFACE" on page 956

Example

This example removes the guest VLAN from ports 1.0.23 and 1.0.24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23,port1.0.24
awplus(config-if)# no auth guest-vlan
```

NO AUTH REAUTHENTICATION

Syntax

```
no auth reauthentication
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove reauthentication from authenticator ports so that supplicants do not have to periodically reauthenticate after the initial authentication. Reauthentication is still required if there is a change to the status of the link between a supplicant and the switch, or the switch is reset or power cycled.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951

"SHOW DOT1X INTERFACE" on page 956

Example

This example deactivates reauthentication on port 1.0.2:

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

NO AUTH-MAC ENABLE

Syntax

```
no auth-mac enable
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to deactivate MAC address-based authentication on authenticator ports.

Confirmation Command

"SHOW DOT1X SUPPLICANT INTERFACE" on page 958

Example

This example removes MAC address-based authentication from port 1.0.23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no auth-mac enable
```

NO DOT1X PORT-CONTROL

Syntax

```
no dot1x port-control
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove ports from the authenticator role so that they forward traffic without authentication.

Confirmation Command

"SHOW AUTH-MAC INTERFACE" on page 951 or "SHOW DOT1X INTERFACE" on page 956

Example

This example removes port 1.0.14 from the authenticator role:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# no dot1x port-control
```

SHOW AUTH-MAC INTERFACE

Syntax

show auth-mac interface *port*

Parameters

port
Specifies a port. You can display more than one port at a time.

Modes

Privileged Exec mode

Description

Use this command to display the parameter settings of the authenticator ports. This command is equivalent to "SHOW DOT1X INTERFACE" on page 956. An example is shown in Figure 158.

```
Authentication Info for interface port1.0.2
   portEnabled: Enabled - portControl: Auto
   portStatus: UP
   reAuthenticate: Disabled
   reAuthPeriod: 3600
   PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
   BE: suppTimeout: 30 - serverTimeout: 30
   CD: adminControlledDirections: both
   criticalVlan: Disabled
   guestVlan: Disabled
   dynamicVlanCreation: None
   hostMode: Single-Host
   dot1x: Enabled
   protocolVersion: 1
   authMac: Enabled
   reAuthRelearning: Disabled
```

Figure 158. SHOW AUTH-MAC INTERFACE Command

Example

This example displays the parameter settings of authenticator ports 1.0.1 through 1.0.4:

awplus# show auth-mac interface port1.0.1-port1.0.4

SHOW AUTH-MAC SESSIONSTATISTICS INTERFACE

Syntax

```
show auth-mac sessionstatistics interface port
```
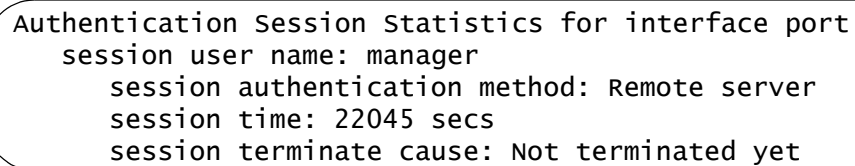
Parameters

port

Specifies a port. You can enter more than one port.

Mode

Privileged Exec mode

Description

Use this command to display session statistics of the authenticator ports. An example is shown in Figure 159.

```
Authentication Session Statistics for interface port
   session user name: manager
      session authentication method: Remote server
      session time: 22045 secs
      session terminate cause: Not terminated yet
```

Figure 159. SHOW AUTH-MAC SESSIONSTATISTICS INTERFACE Command

Example

This example displays the session statistics of the authenticator port 1.0.17:

```
awplus# show auth-mac sessionstatistics interface port1.0.17
```

952

SHOW AUTH-MAC STATISTICS INTERFACE

Syntax

```
show auth-mac statistics interface port
```

Parameters

port
> Specifies a port. You can enter more than one port.

Mode

Privileged Exec mode

Description

Use this command to display EAP packet statistics of authenticator ports. This command is equivalent to "SHOW DOT1X STATISTICS INTERFACE Command" on page 957. An example is shown in Figure 160.

```
Authentication Statistics for interface port1.0.2
    EAPOL Frames Rx: 0 – EAPOL Frames Tx: 0
    EAPOL Start Frames Rx: 0 – EAPOL Logoff Frames Rx: 0
    EAP Rsp/Id Frames Rx: 0 – EAP Response Frames Rx: 0
    EAP Req/Id Frames Tx: 0 – EAP Request Frames Tx: 0
    Invalid EAPOL Frames Rx: 0 – EAP Length Error Frames Rx: 0
    EAPOL Last Frame Version Rx: 0 – EAPOL Last Frame Src: 0000.0000.0000
```

Figure 160. SHOW AUTH-MAC STATISTICS INTERFACE Command

Example

This example displays the EAP packet statistics of authenticator port 1.0.7:

```
awplus# show auth-mac statistics interface port1.0.7
```

SHOW AUTH-MAC SUPPLICANT INTERFACE

Syntax

```
show auth-mac supplicant interface port
```

Parameters

port

Specifies a port. You can enter more than one port.

Mode

Privileged Exec mode

Description

Use this command to display the supplicant state of the authentication mode set for the interface on authenticator ports. This command is equivalent to "SHOW DOT1X SUPPLICANT INTERFACE Command" on page 958. An example is shown in Figure 161.

```
Interface port1.0.3
    authenticationMethod: dot1x
    totalSupplicantNum: 0
    authorizedSupplicantNum: 0
        macBasedAuthenticationSupplicantNum: 0
        dot1xAuthenticationSupplicantNum: 0
        webBasedAuthenticationSupplicantNum: 0
        otherAuthenticationSupplicantNum: 0
No supplicants
```

Figure 161. SHOW AUTH-MAC SUPPLICANT INTERFACE Command

Example

This example displays the supplicant state of the authentication mode on ports 1.0.21 and 1.0.23:

```
awplus# show auth-mac supplicant interface port1.0.21-
port1.0.23
```

SHOW DOT1X

Syntax

show dot1x

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display whether 802.1x port-based network access control is enabled or disabled on the switch and the IP addresses of the RADIUS servers. An example is shown in Figure 162.

```
802.1 Port-Based Authentication: Enabled
   RADIUS server address (auth): 149.32.146.78
```

Figure 162. SHOW DOT1X Command

Example

This example displays the status of the 802.1x port-based network access control feature and the IP addresses of the RADIUS servers:

awplus# show dot1x

SHOW DOT1X INTERFACE

Syntax

```
show dot1x interface port
```

Parameters

port
> Specifies a port. You can display more than one port at a time.

Modes

Privileged Exec mode

Description

Use this command to display the parameter settings of authenticator ports. This command is equivalent to "SHOW AUTH-MAC INTERFACE" on page 951.

Figure 163 displays an example of the information.

```
Authentication Info for interface port1.0.2
portEnabled: Enabled - portControl: Auto
portStatus: UP
reAuthenticate: Enabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: both
guestVlan: Enabled
hostMode: Single-Host
dot1x: Enabled
protocolVersion: 1
authMac: Disabled
reAuthRelearning: Disabled
```

Figure 163. SHOW DOT1X INTERFACE Command

Example

The example displays the authenticator parameter settings for ports 1.0.1 to 1.0.4:

```
awplus> enable
awplus# show dot1x interface port1.0.1-port1.0.4
```

SHOW DOT1X STATISTICS INTERFACE

Syntax

```
show dot1x statistics interface port
```

Parameters

port

Specifies a port. You can enter more than one port.

Mode

Privileged Exec mode

Description

Use this command to display EAP packet statistics of authenticator ports. This command is equivalent to "SHOW AUTH-MAC STATISTICS INTERFACE" on page 953. An example is shown in Figure 164.

```
Authentication Statistics for interface port1.0.2
    EAPOL Frames Rx: 0 – EAPOL Frames Tx: 0
    EAPOL Start Frames Rx: 0 – EAPOL Logoff Frames Rx: 0
    EAP Rsp/Id Frames Rx: 0 – EAP Response Frames Rx: 0
    EAP Req/Id Frames Tx: 0 – EAP Request Frames Tx: 0
    Invalid EAPOL Frames Rx: 0 – EAP Length Error Frames Rx: 0
    EAPOL Last Frame Version Rx: 0 – EAPOL Last Frame Src: 0000.0000.0000
```

Figure 164. SHOW DOT1X STATISTICS INTERFACE Command

Example

This example displays the EAP packet statistics for authenticator port 1.0.7:

```
awplus> enable
awplus# show dot1x statistics interface port1.0.7
```

SHOW DOT1X SUPPLICANT INTERFACE

Syntax

```
show dot1x supplicant interface port [brief]
```

Parameters

port

Specifies a port. You can enter more than one port.

[brief]

Displays an abbreviated form of this window. This is an optional parameter.

Mode

Privileged Exec mode

Description

Use this command to display the supplicant state of the authentication mode set for the interface on authenticator ports. This command is equivalent to "SHOW AUTH-MAC SUPPLICANT INTERFACE Command" on page 954. An example is shown in Figure 165.

```
Interface port1.0.3
  authenticationMethod: dot1x
  totalSupplicantNum: 2
  authorizedSupplicantNum: 2
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 2
    otherAuthenticationSupplicantNum: 0

  Supplicant name: user2
  Supplicant address: 680A.7583.0000
    authenticationMethod: dot1x
    portStatus: Authorized - currentId: 2
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0
    PAE: quietPeriod: 0 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0
    CD: adminControlledDirections: both
```

Figure 165. SHOW DOT1X SUPPLICANT INTERFACE Command

Example

This example displays the supplicant state of the authentication mode on ports 1.0.21 to 1.0.23:

```
awplus> enable
awplus# show dot1x supplicant interface port1.0.21-
port1.0.23
```

Section IX
Simple Network Management Protocols

This section contains the following chapters:

962

Chapter 62

SNMPv1 and SNMPv2c

This chapter contains the following topics:

Overview

The Simple Network Management Protocol (SNMP) is another way for you to monitor and configure the switch. This method lets you view and change the individual objects in the Management Information Base (MIB) in the management software on the switch, without having to use the command line commands.

The switch supports three versions of SNMP— SNMPv1, SNMPv2c, and SNMPv3. This chapter discusses SNMPv1 and SNMPv2c. For information on SNMPv3, refer to Chapter 64, "SNMPv3 Commands" on page 999.

Here are the main steps to using SNMP:

- Load the Allied Telesis MIBs for the switch onto your SNMP management workstation. The MIBs are available from the Allied Telesis web site at **www.alliedtelesis.com**.

A community string must be assigned an access level. The levels are Read and Read/Write. A community string that has an access level of Read can be used to view, but not change, the MIB objects on the switch. A community string that has a Read/Write access level can be used to both view the MIB objects and change them.

The switch can have up to eight community strings. The switch has two default community strings: public and private. The public string has an access level of Read, and the private string has an access mode of Read/Write. If you activate SNMP management on the switch, you should delete the private community string, which is a standard community string in the industry, to protect the switch from unauthorized changes.

The switch can send SNMP trap and inform messages to notify you about device events, such as changes in the states of port links. These messages are sent to receivers on your network. The difference between the messages is that the switch, when it sends inform messages, expects to receive acknowledgements from the receivers, whereas it does not expect acknowledgements when it sends traps.

To configure the switch to send trap or inform messages, you have to add to one or more of the community strings the IP addresses of the trap and inform receivers on your network. For trap messages, you must also specify the format in which the switch should send the messages. The format can be either SNMPv1 or SNMPv2c. For inform messages, the format is always SNMPv2c. For instructions, refer to "Adding or Removing IP Addresses of Trap or Inform Receivers" on page 968.

You can configure SNMPv1 and SNMPv2c with the SNMPv3 Table commands described in Chapter 64, "SNMPv3 Commands" on page 999. However, the SNMPv3 Table commands require a much more extensive configuration.

Enabling SNMPv1 and SNMPv2c

To enable SNMP on the switch, use the SNMP-SERVER command, found in the Global Configuration mode. The command has no parameters. The switch begins to send trap and inform messages to the receivers and permits remote management from SNMP workstations as soon as you enter the command. This assumes, of course, you have already created the community strings and added the IP addresses of trap and inform receivers. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server
```

Creating Community Strings

To create SNMPv1 and SNMPv2c community strings, use the SNMP-SERVER COMMUNITY command. This command is found in the Global Configuration mode. Here is the format of the command:

```
snmp-server community community rw|ro
```

You can create only one string at a time with the command. The COMMUNITY parameter is the name of the new string. It can be up to 15 alphanumeric characters and special characters, such as, !@#$%^&*?<>, and is case sensitive. Spaces are not allowed.

The RW and RO options define the access levels of new community strings. RW is read-write and RO is read-only.

This example creates the community string "plarnum" with read-write access:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server community plarnum rw
```

This example creates the community string "station5b2" with read-only access:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server community station5b2 ro
```

Adding or Removing IP Addresses of Trap or Inform Receivers

The command to add IP addresses of trap or inform receivers to community strings is the SNMP-SERVER HOST command. Here is the format:

```
snmp-server host ipaddress traps|informs version 1|2c
community
```

The IPADDRESS parameter is the IP address of a receiver. The COMMUNITY parameter is an existing community string to which you want to add the address. The community string is case sensitive.

The TRAPS and INFORMS parameters control whether or not the switch expects to receive acknowledgements from your SNMP applications after it sends the messages. Acknowledgements are expected for inform messages, but not for trap messages.

The 1 and 2C parameters define the format of the trap messages. The switch can send trap messages in either SNMPv1 or SNMPv2c format. Inform messages can only be sent in SNMPv2c format.

Note
SNMP must be activated on the switch for you to add trap or inform receivers to community strings. To activate SNMP, use the SNMP-SERVER command in the Global Configuration mode.

This example activates SNMP on the switch and assigns the IP address 121.12.142.8 as a trap receiver to the private community string. The messages are sent in SNMPv2c format:

```
awplus> enable
awplus# configure terminal
awplus# snmp-server
awplus(config)# snmp-server host 121.12.142.8 trap version
2c private
```

The rest of the examples assume that SNMP is already activated on the switch and so omit the SNMP-SERVER command.

This example assigns the IP address 121.14.154.11 as a trap receiver to the community string "Wanpam." The messages are sent in SNMPv1 format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 121.14.154.11 trap version
1 Wanpam
```

This example assigns the IP address 143.154.76.17 as an inform message receiver to the community string "st_bldg2." Inform messages must be sent in SNMPv2c format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 143.154.76.17 informs
version 2c st_bldg2
```

To remove IP addresses of trap or inform receivers from community strings, use the NO form of the command. This example removes the IP address 121.12.142.8 of a trap receiver from the private community string:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 121.12.142.8 trap
version 2c private
```

969

Deleting Community Strings

To delete community strings, use the NO SNMP-SERVER COMMUNITY command. Here is the format:

```
no snmp-server community community
```

You can delete only one community string at a time with the command, which is found in the Global Configuration mode. The COMMUNITY parameter is case sensitive.

This example deletes the "ytnar12a" community string from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server community ytnar12a
```

Disabling SNMPv1 and SNMPv2c

To disable SNMP on the switch, use the NO SNMP-SERVER command. You cannot remotely manage the switch with an SNMP application when SNMP is disabled. Furthermore, the switch stops transmitting trap and inform messages to your SNMP applications. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server
```

Displaying SNMPv1 and SNMPv2c

To learn whether SNMP is enabled or disabled on the switch, go to the Privileged Exec mode and issue the SHOW SNMP-SERVER command:

awplus# show snmp-server

Here is an example of what is displayed.

```
SNMP Server ....... Enabled
IP Protocol ....... IPv4
SNMPv3 Engine ID (Configured) ........ Not set
SNMPv3 Engine ID (actual) ............ 0x80001f8880241d7f08386d438e
```

Figure 166. SHOW SNMP-SERVER Command

The status of SNMP is displayed in the first field as either Enabled or Disabled. (The other fields in the window are not applicable to SNMPv1 and SNMPv2c.)

To view the community strings on the switch, use the SHOW SNMP-SERVER COMMUNITY command:

awplus# show snmp-server community

Here is an example of the information the command displays:

```
SNMP community information:
    Community Name .............. sw12eng1
        Access .................. Read-Write
        View .................... None
    Community Name .............. sw12eng1limit
        Access .................. Read-only
        View .................... None
    Community Name .............. westplnm7
        Access .................. Read-only
        View .................... None
    Community Name .............. site12pl4
        Access .................. Read-only
        View .................... None
```

Figure 167. SHOW SNMP-SERVER COMMUNITY Command

The information that the command provides for each community string includes the community name and the access level of read-write or read-only. There is also a view field which, for community strings created through the SNMPv1 and SNMPv2c commands, always has a value of None, indicating that the strings give an SNMP application access to the entire MIB tree of the switch. SNMPv1 and SNMPv2c community strings created with SNMPv3 can be configured so that they are restricted to particular parts of the MIB tree.

972

To view the trap and inform receivers assigned to the community strings, use the SHOW RUNNING-CONFIG SNMP command in the Privileged Exec mode:

awplus# show running-config snmp

Here is an example of command display:

```
snmp-server
no snmp-server enable trap auth
snmp-server community sw12eng1 rw
snmp-server community sw12eng1limit rw
snmp-server community westplnm7 ro
snmp-server community site12pl4 ro
snmp-server host 149.198.74.143 traps version 2c sw12eng1
snmp-server host 149.198.74.154 traps version 2c sw12eng1
snmp-server host 149.198.121.17 traps version 2c sw12eng1limit
snmp-server host 149.198.121.198 traps version 2c sw12eng1limit
```

Figure 168. SHOW RUNNING-CONFIG SNMP Command

Chapter 63

SNMPv1 and SNMPv2c Commands

The SNMPv1 and SNMPv2c commands are summarized in Table 88 and described in detail within the chapter.

Table 88. SNMPv1 and SNMPv2c Commands

Command	Mode	Description
"NO SNMP-SERVER" on page 977	Global Configuration	Disables SNMPv1 and SNMPv2c on the switch.
"NO SNMP-SERVER COMMUNITY" on page 978	Global Configuration	Deletes SNMPv1 and SNMPv2c community strings.
"NO SNMP-SERVER ENABLE TRAP" on page 979	Global Configuration	Disables the transmission of all SNMP traps, except for link status and authentication traps, which are disabled separately.
"NO SNMP-SERVER ENABLE TRAP AUTH" on page 980	Global Configuration	Disables the transmission of SNMP authentication traps.
"NO SNMP-SERVER HOST" on page 981	Global Configuration	Removes the IP addresses of trap and inform receivers from the community strings.
"NO SNMP-SERVER VIEW" on page 983	Global Configuration	Deletes SNMP views.
"NO SNMP TRAP LINK-STATUS" on page 984	Port Interface	Disables the transmission of SNMP link status notifications when ports establish links or lose links to network devices.
"SHOW RUNNING-CONFIG SNMP" on page 985	Privileged Exec	Displays the SNMPv1 and v2c community strings and the IP addresses of trap and inform receivers.
"SHOW SNMP-SERVER" on page 986	Privileged Exec	Displays the current status of SNMP on the switch.
"SHOW SNMP-SERVER COMMUNITY" on page 987	Privileged Exec	Displays the status of SNMPv1 and SNMPv2c and the community strings.

975

Table 88. SNMPv1 and SNMPv2c Commands (Continued)

Command	Mode	Description
"SHOW SNMP-SERVER VIEW" on page 989	Privileged Exec	Displays the SNMP views.
"SNMP-SERVER" on page 990	Global Configuration	Enables SNMPv1 and SNMPv2c on the switch.
"SNMP-SERVER COMMUNITY" on page 991	Global Configuration	Creates new SNMPv1 and SNMPv2c community strings.
"SNMP-SERVER ENABLE TRAP" on page 992	Global Configuration	Activates the transmission of all SNMP traps, except for link status and authentication traps, which are activated separately.
"SNMP-SERVER ENABLE TRAP AUTH" on page 993	Global Configuration	Activates the transmission of SNMP authentication traps.
"SNMP-SERVER HOST" on page 994	Global Configuration	Adds the IP addresses of trap and informs receivers to the community strings on the switch.
"SNMP-SERVER VIEW" on page 996	Global Configuration	Creates SNMP views.
"SNMP TRAP LINK-STATUS" on page 998	Port Interface	Configures SNMP to transmit link status notifications when ports establish links or lose links to network devices.

NO SNMP-SERVER

Syntax

```
no snmp-server
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable SNMPv1, SNMPv2c and SNMPv3 on the switch. The switch does not permit remote management from SNMP applications when SNMP is disabled. It also does not send SNMP trap or inform messages.

Confirmation Command

"SHOW SNMP-SERVER" on page 986.

Example

This example disables SNMPv1, SNMPv2c, or SNMPv3 on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server
```

NO SNMP-SERVER COMMUNITY

Syntax

```
no snmp-server community community
```

Parameter

community
> Specifies an SNMP community string to be deleted from the switch. This parameter is case sensitive.

Mode

Global Configuration mode

Description

Use this command to delete SNMPv1 and SNMPv2c community strings from the switch. Deleting community strings with this command also deletes any IP addresses of SNMP trap or inform receivers assigned to the community strings. You can delete only one community string at a time with this command.

Confirmation Command

"SHOW SNMP-SERVER COMMUNITY" on page 987

Example

This example deletes the "pla178ta" community string from the switch, as well as any IP addresses of trap or inform receivers that are assigned to it:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server community pla178ta
```

NO SNMP-SERVER ENABLE TRAP

Syntax

```
no snmp-server enable trap
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the transmission of SNMP traps, except for the link status and authentication traps, which are disabled separately.

Confirmation Command

"SHOW RUNNING-CONFIG SNMP" on page 985

Example

This example disables the transmission of all SNMP traps, except for the link status and authentication traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server enable trap
```

NO SNMP-SERVER ENABLE TRAP AUTH

Syntax

```
no snmp-server enable trap auth
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the transmission of SNMP traps.

Confirmation Command

"SHOW RUNNING-CONFIG SNMP" on page 985

Example

This example disables the transmission of SNMP traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server enable trap auth
```

NO SNMP-SERVER HOST

Syntax

```
no snmp-server host ipaddress traps|informs version 1|2c
community_string
```

Parameters

ipaddress

Specifies the IPv4 or IPv6 address of a trap or inform receiver to be removed from a community string. You can specify only one IP address.

traps|informs

Specifies the type of messages the switch is sending to the receiver.

1|2c

Specifies the format of the messages that the switch is transmitting to the receiver. You can specify only 2c when you are deleting the IP address of an inform message receiver.

community_string

Specifies the SNMP community string to which the IP address of the trap or inform receiver is assigned. This parameter is case sensitive.

Mode

Global Configuration mode

Description

Use this command to remove IP addresses of trap or inform receivers from the community strings on the switch. You can remove only one receiver at a time with this command. The switch does not send any further SNMP trap or inform messages to network devices after their IP addresses have been deleted from the community strings.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example removes the IPv4 address 115.124.187.4 of a trap receiver from the private community string:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 115.124.187.4 traps
version 1 private
```

This example removes the IPv4 address 171.42.182.102 of a trap receiver from the community string "station12a":

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 115.124.187.4 traps
version 2c station12a
```

This example removes the IPv6 address 124c:75:ae3::763:8b4 of an inform receiver from the community string "wadt27:"

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 124c:75:ae3::763:8b4
informs version 2c wadt27
```

982

NO SNMP-SERVER VIEW

Syntax

```
no snmp-server view viewname oid
```

Parameters

viewname

Specifies the name of the view to be deleted. The name is case sensitive.

oid

Specifies the OID of the view.

Mode

Global Configuration mode

Description

Use this command to delete SNMP views. You can delete just one view at a time with this command.

Confirmation Command

"SHOW SNMP-SERVER VIEW" on page 989

Example

This example deletes the view AlliedTelesis with the OID 1.3.6.1.4.1.207:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server view AlliedTelesis
1.3.6.1.4.1.207
```

NO SNMP TRAP LINK-STATUS

Syntax

```
no snmp trap link-status
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the transmission of SNMP link status notifications (traps) when ports establish links (linkUp) or lose links (linkDown) to network devices.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example disables the transmission of link status notifications on ports 17 and 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17,port1.0.21
awplus(config-if)# no snmp trap link-status
```

984

SHOW RUNNING-CONFIG SNMP

Syntax

```
show running-config snmp
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv1 and SNMPv2c community strings and the IP addresses of trap and inform receivers. An example is shown in Figure 169.

```
snmp-server
no snmp-server enable trap auth
snmp-server community sw12eng1 rw
snmp-server community sw12eng1limit rw
snmp-server community westplnm7 ro
snmp-server community site12pl4 ro
snmp-server host 149.198.74.143 traps version 2c sw12eng1
snmp-server host 149.198.74.154 traps version 2c sw12eng1
snmp-server host 149.198.121.17 traps version 2c sw12eng1limit
snmp-server host 149.198.121.198 traps version 2c sw12eng1limit
```

Figure 169. SHOW RUNNING-CONFIG SNMP Command

Example

This example displays the SNMPv1 and SNMPv2c community strings and the IP addresses of trap and inform receivers:

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

SHOW SNMP-SERVER

Syntax

show snmp-server

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the current status of SNMP on the switch. An example is shown in Figure 170. The first field displays whether SNMP is enabled or disabled on the switch. You can remotely manage the switch with SNMPv1 or v2c when the server is enabled. Remote management is not possible when the server is disabled. To activate or deactivate SNMP, refer to "SNMP-SERVER" on page 990 and "NO SNMP-SERVER" on page 977, respectively.

```
SNMP Server ....... Enabled
IP Protocol ....... IPv4
SNMPv3 Engine ID (Configured) ........ Not set
SNMPv3 Engine ID (actual) ............ 0x80001f8880241d7f08386d438e
```

Figure 170. SHOW SNMP-SERVER Command

Example

This example displays the current status of SNMP on the switch:

awplus# show snmp-server

SHOW SNMP-SERVER COMMUNITY

Syntax

show snmp-server community

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv1 and SNMPv2c community strings on the switch. Here is an example of the display.

```
SNMP community information:
    Community Name ............. private
        Access .................. Read-Write
        View .................... None
    Community Name ............. public
        Access .................. Read-only
        View .................... None
```

Figure 171. SHOW SNMP-SERVER COMMUNITY Command

The fields in the entries are described in Table 89.

Table 89. SHOW SNMP-SERVER COMMUNITY Command

Parameter	Description
Community Name	The community string.
Access	The access level of the community string. The possible access levels are Read-Write and Read-Only.
View	The name of an SNMP view that defines a portion of the MIB tree that the community string is not permitted to access. Community strings that are not assigned views have a value of None, which means they have access to the entire MIB tree.

Example

This example displays the SNMPv1 and SNMPv2c community strings:

```
awplus# show snmp-server community
```

SHOW SNMP-SERVER VIEW

Syntax

```
show snmp-server view
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv1 and SNMPv2c views on the switch. Here is an example of the display.

```
SNMP View information:
   View Name ............. system
      OID ................ 1.3.6.12.1.1
      Type .............. excluded
   View Name ............. AlliedTelesis
      OID ................ 1.3.6.1.4.1.207
      Type .............. excluded
```

Figure 172. SHOW SNMP-SERVER VIEW Command

The fields in the entries are described in Table 90.

Table 90. SHOW SNMP-SERVER VIEW Command

Parameter	Description
View Name	The view name.
OID	The OID to a section of the MIB tree.
Type	The view type, which is always excluded.

Example

This example displays the SNMPv1 and SNMPv2c views on the switch:

```
awplus# show snmp-server view
```

SNMP-SERVER

Syntax

```
snmp-server
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate SNMPv1, SNMPv2c and SNMPv3 on the switch. The switch permits remote management from SNMP applications when SNMP is enabled. The switch also sends SNMP messages to trap and inform receivers.

Confirmation Command

"SHOW SNMP-SERVER" on page 986

Example

This example activates SNMPv1, SNMPv2c or SNMPv3 on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server
```

SNMP-SERVER COMMUNITY

Syntax

```
snmp-server community community rw|ro
```

Parameters

community

Specifies a new community string. The maximum length is 40 alphanumeric and/or special characters, such as, !@#$%^&*?<>. The name is case sensitive. Spaces are not allowed.

rw|ro

Specifies the access level of a new community string, of read-write (RW) or read-only (RO).

Mode

Global Configuration mode

Description

Use this command to create new SNMPv1 and SNMPv2c community strings on the switch. The switch can have up to eight community strings.

Confirmation Command

"SHOW SNMP-SERVER COMMUNITY" on page 987

Example

This example creates the new community string "stea2a," with an access level of read-write:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server community stea2a rw
```

991

SNMP-SERVER ENABLE TRAP

Syntax

```
snmp-server enable trap
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the transmission of all SNMP traps, except for power-inline, link status, and authentication traps, which are activated separately.

Confirmation Command

"SHOW RUNNING-CONFIG SNMP" on page 985

Example

This example activates the transmission of all SNMP traps, except for power-inline, link status, and authentication traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server enable trap
```

SNMP-SERVER ENABLE TRAP AUTH

Syntax

```
snmp-server enable trap auth
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the transmission of SNMP authentication failure traps.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example activates the transmission of SNMP authentication failure traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server enable trap auth
```

SNMP-SERVER HOST

Syntax

```
snmp-server host ipaddress traps|informs version 1|2c
community
```

Parameters

ipaddress

Specifies the IPv4 or IPv6 address of a network device to receive trap or inform messages from the switch.

traps|informs

Specifies the type of messages.

1|2c

Specifies the format of the traps sent by the switch. For trap messages, the format can be SNMPv1 (1) or SNMPv2c (2c). For inform messages, the format must be SNMPv2c (2c).

community

Specifies an SNMP community string. This parameter is case sensitive.

Mode

Global Configuration mode

Description

Use this command to specify IP addresses of network devices to receive trap and inform messages from the switch. A community string can have up to eight IP addresses of trap and inform receivers.

SNMP must be enabled on the switch for you to add trap and inform receivers to community strings. To enable SNMP, refer to "SHOW SNMP-SERVER VIEW" on page 989

Confirmation Command

"SHOW RUNNING-CONFIG SNMP" on page 985

Examples

This example assigns the IPv4 address 149.44.12.44 of a trap receiver to the private community string. The traps are sent in the SNMPv2c format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 149.44.12.44 traps version
2c private
```

This example assigns the IPv4 address 152.34.32.18 as a trap receiver to the community string "tlpaac78". The traps are sent in the SNMPv1 format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 152.34.32.18 traps version
1 tlpaac78
```

This example assigns the IPv6 address 45ac:be22:78::c45:8156 as an inform receiver to the community string "anstat172". Inform messages must be sent in the SNMPv2c format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 45ac:be22:78::c45:8165
informs version 2c anstat172
```

SNMP-SERVER VIEW

Syntax

```
snmp-server view viewname oid excluded|included
```

Parameters

viewname
> Specifies the name of a new view. The maximum length is 64 alphanumeric and/or special characters. The string is case sensitive. Spaces are not allowed.

oid
> Specifies the OID of the view. The OID must be in decimal format.

excluded
> Denies access to the part of the MIB tree specified by the OID.

included
> Permits access to the part of the MIB tree specified by the OID.

Mode

Global Configuration mode

Description

Use this command to create SNMPv1 and SNMPv2c views on the switch. Views are used to restrict the MIB objects that network managers can access through the community strings. A view can have more than one OID, but each OID must be entered in a separate command.

Confirmation Command

"SHOW SNMP-SERVER VIEW" on page 989

Examples

This example creates a view that excludes all MIB objects in the OID 1.3.6.1.2.1. The view is assigned the name "sw12_restrict_view:"

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view sw12_restrict_view
1.3.6.1.2.1 excluded
```

996

This example creates the new view "AlliedTelesis" that limits the available MIB objects to those in the OID 1.3.6.1.4.1.207:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view AlliedTelesis 1.3.6.1
excluded
awplus(config)# snmp-server view AlliedTelesis
1.3.6.1.4.1.207 included
```

SNMP TRAP LINK-STATUS

Syntax

```
snmp trap link-status
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable SNMP to transmit link status notifications (traps) when ports establish links (linkUp) or lose links (linkDown) to network devices.

Confirmation Command

"SHOW INTERFACE" on page 221

Example

This example configures the switch to transmit link status notifications whenever links are established or lost on ports 1 to 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# snmp trap link-status
```

Chapter 64
SNMPv3 Commands

The SNMPv3 commands are summarized in Table 91 and described in detail within the chapter.

Table 91. SNMPv3 Commands

Command	Mode	Description
"NO SNMP-SERVER" on page 1001	Global Configuration	Disables SNMPv1, v2c and v3 on the switch.
"NO SNMP-SERVER ENGINEID LOCAL" on page 1002	Global Configuration	Returns the SNMP engine ID value to the default value:
"NO SNMP-SERVER GROUP" on page 1003	Global Configuration	Deletes SNMPv3 groups from the switch.
"NO SNMP-SERVER HOST" on page 1004	Global Configuration	Deletes SNMPv3 host entries.
"NO SNMP-SERVER USER" on page 1006	Global Configuration	Deletes SNMPv3 users from the switch.
"NO SNMP-SERVER VIEW" on page 1007	Global Configuration	Deletes SNMPv3 views from the switch.
"SHOW SNMP-SERVER" on page 1008	Privileged Exec	Displays the current status of SNMP on the switch.
"SHOW SNMP-SERVER GROUP" on page 1009	Privileged Exec	Displays the SNMPv3 groups.
"SHOW SNMP-SERVER HOST" on page 1010	Privileged Exec	Displays SNMPv3 host entries.
"SHOW SNMP-SERVER USER" on page 1011	Privileged Exec	Displays SNMPv3 users.
"SHOW SNMP-SERVER VIEW" on page 1012	Privileged Exec	Displays SNMPv3 views.
"SNMP-SERVER" on page 1013	Global Configuration	Activates SNMPv1, v2c and v3 on the switch.
"SNMP-SERVER ENGINEID LOCAL" on page 1014	Global Configuration	Configures the SNMPv3 engine ID.

Table 91. SNMPv3 Commands (Continued)

Command	Mode	Description
"SNMP-SERVER GROUP" on page 1015	Global Configuration	Creates SNMPv3 groups.
"SNMP-SERVER HOST" on page 1017	Global Configuration	Creates SNMPv3 host entries.
"SNMP-SERVER USER" on page 1019	Global Configuration	Creates SNMPv3 users.
"SNMP-SERVER VIEW" on page 1021	Global Configuration	Creates SNMPv3 views.

NO SNMP-SERVER

Syntax

```
no snmp-server
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable SNMPv1, SNMPv2c, and SNMPv3 on the switch. The switch does not permit remote management from SNMP applications when SNMP is disabled. It also does not send SNMP trap or inform messages.

Confirmation Command

"SHOW SNMP-SERVER" on page 1008.

Example

This example disables SNMPv1, SNMPv2c, or SNMPv3 on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server
```

NO SNMP-SERVER ENGINEID LOCAL

Syntax

```
no snmp-server engineid local
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to return the SNMP engine ID value to the default value.

Confirmation Command

"SHOW SNMP-SERVER" on page 1008

Example

This example returns the SNMP engine ID value to the default value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server engineid local
```

NO SNMP-SERVER GROUP

Syntax

```
no snmp-server group name noauth|auth|priv
```

Parameters

name

Specifies the name of a group you want to delete from the switch. The name is case sensitive.

auth/noauth/priv

Specifies the minimum security level of the group to be deleted. The options are:

auth: Indicates authentication, but no privacy.

noauth: Indicates no authentication or privacy.

priv: Indicates authentication and privacy.

Mode

Global Configuration mode

Description

Use this command to delete SNMPv3 groups.

Confirmation Command

"SHOW SNMP-SERVER GROUP" on page 1009

Example

This example deletes the SNMPv3 group "campus1_mgmt" with authentication and privacy security:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server group campus1_mgmt priv
```

NO SNMP-SERVER HOST

Syntax

```
no snmp-server host ipaddress informs/traps v3
auth/noauth/priv username
```

Parameters

ipaddress

> Specifies the IP address of a trap receiver. The address can be IPv4 or IPv6. You can specify just one address.

informs/trap

> Specifies the type of message the switch sends. The options are:
>
> > *informs:* Sends inform messages.
> >
> > *trap:* Sends trap messages.

noauth/auth/priv

> Specifies the minimum security level of the user associated with this entry. The options are:
>
> > *noauth:* Indicates no authentication or privacy.
> >
> > *auth:* Indicates authentication, but no privacy.
> >
> > *priv:* Indicates authentication and privacy.

username

> Specifies an SNMPv3 user name.

Mode

Global Configuration mode

Description

Use this command to delete SNMPv3 host entries. Host entries define the IP addresses to receive SNMPv3 inform and trap messages.

Example

This example deletes the host entry with the IPv4 address 187.87.165.12. The user name associated with this entry is "jones:"

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 187.87.165.12 traps v3 auth
jones
```

NO SNMP-SERVER USER

Syntax

```
no snmp-server user user
```

Parameters

user

Specifies the name of a user you want to delete from the switch. The name is case sensitive.

Mode

Global Configuration mode

Description

Use this command to delete SNMPv3 users. You can delete just one user at a time with this command.

Confirmation Command

"SHOW SNMP-SERVER USER" on page 1011

Example

This example deletes the SNMPv3 user "tedwards":

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server user tedwards
```

NO SNMP-SERVER VIEW

Syntax

```
no snmp-server view view OID
```

Parameters

view

Specifies the name of a view to be deleted from the switch. The name is case sensitive.

OID

Specifies the OID of the subtree of the view to be deleted.

Mode

Global Configuration mode

Description

Use this command to delete SNMPv3 views from the switch.

Confirmation Command

"SHOW SNMP-SERVER VIEW" on page 1012

Example

This example deletes the view All, which has the OID 1.3.6.1:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view All subtree 1.3.6.1
```

SHOW SNMP-SERVER

Syntax

show snmp-server

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the current status of SNMP on the switch. An example is shown in Figure 173. The first field displays whether SNMP is enabled or disabled on the switch. You can remotely manage the switch with SNMPv1 or v2c when the server is enabled. Remote management is not possible when the server is disabled. To activate or deactivate SNMP, refer to "SNMP-SERVER" on page 1013 and "NO SNMP-SERVER" on page 1001, respectively.

```
SNMP Server ....... Enabled
IP Protocol ....... IPv4
SNMPv3 Engine ID (Configured) ........ Not set
SNMPv3 Engine ID (actual) ............ 0x80001f8880241d7f08386d438e
```

Figure 173. SHOW SNMP-SERVER Command

Example

This example displays the current status of SNMP on the switch:

awplus# show snmp-server

SHOW SNMP-SERVER GROUP

Syntax

```
show snmp-server group
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv3 groups.

Example

This example displays the SNMPv3 groups:

```
awplus# show snmp-server group
```

SHOW SNMP-SERVER HOST

Syntax

```
show snmp-server host
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv3 host entries.

Example

This example displays the SNMPv3 host entries:

```
awplus# show snmp-server host
```

SHOW SNMP-SERVER USER

Syntax

```
show snmp-server user
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv3 users.

Example

This example displays the SNMPv3 users:

```
awplus# show snmp-server user
```

SHOW SNMP-SERVER VIEW

Syntax

```
show snmp-server view
```

Parameter

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv3 views on the switch.

Example

This example displays the SNMPv3 views on the switch:

```
awplus# show snmp-server view
```

SNMP-SERVER

Syntax

```
snmp-server
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate SNMPv1, SNMPv2c, and SNMPv3 on the switch. The switch permits remote management from SNMP applications when SNMP is enabled. The switch also sends SNMP messages to trap and inform receivers.

Confirmation Command

"SHOW SNMP-SERVER" on page 1008

Example

The following example activates SNMPv1, SNMPv2c, and SNMPv3 on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server
```

SNMP-SERVER ENGINEID LOCAL

Syntax

```
snmp-server engineid local engine-id/default
```

Parameters

engine-id
> Specifies the SNMPv3 engine ID. The value can be up to 32 characters.

default
> Returns the SNMPv3 engine ID to the system-generated value.

Mode

Global Configuration mode

Description

Use this command to configure the SNMPv3 engine ID.

Note
Changing the SNMPv3 engine ID from its default value is not recommended because the SNMP server on the switch may fail to operate properly.

Confirmation Command

"SHOW SNMP-SERVER" on page 1008

Examples

This example sets the SNMPv3 engine ID to 89ab532d782:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server engineid local 89ab532d782
```

This example returns the SNMPv3 engine ID to the default setting:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server engineid local default
```

SNMP-SERVER GROUP

Syntax

```
snmp-server group name auth|noauth|priv read readview|
write writeview
```

Parameters

name

Specifies a name for a new group. A name can be up to 64 alphanumeric and/or special characters, such as, !@#$%^&*?<>, and is case sensitive.

auth/noauth/priv

Specifies the minimum security level that users must have to gain access to the switch through the group. The options are:

auth: Indicates authentication, but no privacy.

noauth: Indicates no authentication or privacy.

priv: Indicates authentication and privacy.

readview

Specifies the name of an existing SNMPv3 view that specifies the MIB objects the members of the group can view. If this parameter is omitted, the members cannot view any MIB objects using the group. The name is case sensitive.

writeview

Specifies the name of an existing SNMPv3 view that specifies the part of the MIB tree the members of the group can change. If this parameter is omitted, the members cannot change any MIB objects using the group. The name is case sensitive.

Mode

Global Configuration Mode

Description

Use this command to create SNMPv3 groups.

Examples

This example creates a group called "sta5west" with a minimum security level of privacy. The group has a read view named "internet" and a write view named "private":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server group sta5west priv read
internet write private
```

This example creates a group called "swengineering" with a minimum security level of authentication and privacy. The group has the read view "internet" and the write view "ATI":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server group swengineering priv read
internet write ATI
```

This example creates a group called "hwengineering" with a security level of no authentication or privacy.The group has the read view "internet," but no write view.

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server group hwengineering noauth read
internet
```

1016

SNMP-SERVER HOST

Syntax

```
snmp-server host ipaddress informs|traps version 3
auth|noauth|priv username
```

Parameters

ipaddress
> Specifies the IP address of a trap receiver. The address can be IPv4 or IPv6. You can specify just one address.

informs/trap
> Specifies the type of message the switch sends. The options are:

> > *informs:* Sends inform messages.

> > *traps:* Sends trap messages.

noauth/auth/priv
> Specifies the minimum security level of the user associated with this entry. The options are:

> > *noauth:* Indicates no authentication or privacy.

> > *auth:* Indicates authentication, but no privacy.

> > *priv:* Indicates authentication and privacy.

username
> Specifies an SNMPv3 user name.

Mode

Global Configuration mode

Description

Use this command to designate network devices to receive SNMPv3 inform and trap messages.

Example

This example configures SNMPv3 to send trap messages to an end node with the IPv4 address 149.157.192.12. The user name associated with this entry is "sthompson:"

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 149.157.192.12 traps
version 3 auth sthompson
```

SNMP-SERVER USER

Syntax

```
snmp-server user username groupname [auth sha|md5
auth_password] [priv des priv_password]
```

Parameters

username

    Specifies a name for a new SNMPv3 user. A name can have up to 32 alphanumeric and/or special characters and is case sensitive. Spaces are not allowed.

groupname

    Specifies a name of a group for a new user. A group name can have up to 32 alphanumeric and/or special characters and is case sensitive. Spaces are not allowed.

auth

    Specifies an authentication protocol for a user. The options are:

        md5: The MD5 Message Digest Algorithms authentication protocol.

        sha: The SHA Secure Hash Algorithms authentication protocol.

auth_password

    Specifies a password for authentication. A password can have up to 40 alphanumeric and/or special characters and is case sensitive. Spaces are not allowed.

priv_password

    Specifies a password for privacy with the 3DES Data Encryption Standard. A password can have up to 40 alphanumeric and/or special characters and is case sensitive.

Mode

Global Configuration mode

Description

Use this command to create new SNMPv3 users. A new user can have a security level of no security, authentication only, or authentication and privacy. The security level is assigned in the following manner:

❒   To create a user that has neither authentication nor privacy, omit both the AUTH and PRIV keywords.

1019

❐ To create a user that has authentication but not privacy, include the AUTH keyword but not the PRIV keyword.

❐ To create a user that has both authentication and privacy, include both the AUTH and PRIV keywords.

You cannot create a user that has privacy but not authentication.

Confirmation Command

"SHOW SNMP-SERVER USER" on page 1011

Examples

This example creates the user "dcraig". The user is not given authentication or privacy:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server user dcraig
```

This example creates the user "bjones". The user is assigned authentication using SHA and the authentication password "as11fir". The account is not assigned privacy:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server user bjones auth sha as11fir
```

This example creates a user with the name "csmith". The account is given both authentication and privacy. The authentication protocol is MD5, the authentication password "light224aq", and the privacy password "pl567pe":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server user csmith auth md5 light224aq
priv des pl567pe
```

SNMP-SERVER VIEW

Syntax

```
snmp-server view viewname oid excluded/included
```

Parameters

viewname

Specifies the name of a new view. The maximum length is 64 alphanumeric and/or special characters. The string is case sensitive. Spaces are not allowed.

oid

Specifies the OID of the view. The OID must be in decimal format. Each decimal equals 1 character, for example, 1.3.6.1.1 would be equivalent to 9 characters.

excluded

Denies access to the part of the MIB tree specified by the OID.

included

Permits access to the part of the MIB tree specified by the OID.

Mode

Global Configuration mode

Description

Use this command to create SNMPv3 views on the switch. Views are used to restrict the MIB objects that network managers can access through SNMPv3 groups. A view can have more than one OID, but each OID must be added in a separate command.

Confirmation Command

"SHOW SNMP-SERVER VIEW" on page 1012

Examples

This example creates a view that excludes all MIB objects in the OID 1.3.6.1.2.1. The view is assigned the name "sw12_restrict_view:"

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view sw12_restrict_view
1.3.6.1.2.1 excluded
```

This example creates the new view "AlliedTelesis" that limits the available MIB objects to those in the OID 1.3.6.1.4.1.207:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view AlliedTelesis 1.3.6.1
excluded
awplus(config)# snmp-server view AlliedTelesis
1.3.6.1.4.1.207 included
```

Section X
Network Management

This section contains the following chapters:

1024

Chapter 65
sFlow Agent

This chapter contains the following topics:

Overview

The sFlow agent allows the switch to gather data about the traffic on the ports and to send the data to an sFlow collector on your network for analysis. You can use the information to monitor the performance of your network or identify traffic bottlenecks.

The sFlow agent can gather two types of information about the traffic on the ports of the switch:

❏ Ingress packet samples

❏ Packet counters

Ingress Packet Samples

The sFlow agent can capture ingress packets on ports and send copies of the packets to an sFlow collector on your network for analysis. Depending on the capabilities of a collector, packets can be scrutinized for source and destination MAC or IP addresses, protocol type, length, and so forth.

Packet sampling is activated by specifying sampling rates on the ports. This value defines the average number of ingress packets from which the agent samples one packet. For example, a sampling rate of 1000 on a port prompts the agent to send one packet from an average of 1000 ingress packets to the designated sFlow collector. Different ports can have different rates.

Packet Counters

The agent can also gather and send data to a collector about overall information regarding the status and performance of the ports, such as speeds and status, and the statistics from the packet counters. The counters contain the number and types of ingress and egress packets handled by the ports since the switch or the counters were last reset. Here is the port status and counter information the agent can gather and send to a collector on your network:

❏ Port number

❏ Port type

❏ Speed

❏ Direction

❏ Status

❏ Number of ingress and egress octets

❏ Number of ingress and egress unicast packets

❏ Number of ingress and egress multicast packets

❏ Number of ingress and egress broadcast packets

❏ Number of ingress and egress discarded packets

❐ Number of ingress and egress packets with errors

❐ Number of ingress packets with unknown protocols

To configure the agent to forward these port statistics to a collector, you have to specify polling rates, which define the maximum amount of time permitted between successive queries of the counters of a port by the agent.

Different ports can have different polling rates. Ports to which critical network devices are connected may be assigned low polling rates, so that the information on the collector is kept up-to-date. Ports connected to less critical devices may be assigned higher polling rates.

To increase its efficiency, the agent may send port status and counter information before the polling interval of a port times out. For example, if you define a polling interval of five minutes for a port, the agent, depending on its internal dynamics, may send the information to the collector before five minutes have actually elapsed.

Guidelines

Here are the guidelines to the sFlow agent.

❐ You can specify just one sFlow collector.

❐ The switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ If the sFlow collector is not a member of the same subnet as the management IP address of the switch, the switch must be able to access the subnet in which the collector is located, through routers or other Layer 3 devices.

❐ If the sFlow collector is not a member of the same subnet as the management IP address of the switch, the switch must have a default gateway that specifies the first hop to reaching the collector's subnet. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ This feature is not dependent on SNMP. You do not have to enable or configure SNMP on the switch to use it. Additionally, you cannot use an sFlow collector with SNMP to configure or manage this feature.

Configuring the sFlow Agent

The command for defining the IP address of the sFlow collector is the SFLOW COLLECTOR IP command. The command, which is located in the Global Configuration mode, has this format:

sflow collector ip *ipaddress* port *udp_port*

The IPADDRESS parameter specifies the IP address of the collector and the UDP_PORT parameter its UDP port. This example specifies the IP address of the sFlow collector as 154.122.11.24 and the UDP port as 6300:

```
awplus> enable
awplus# configure terminal
awplus(config)# sflow collector ip 154.122.11.24 port 6300
```

After configuring the agent, go to the next section to configure the ports whose performance data is to be sent to the collector.

Configuring the Ports

To configure the ports so that their performance data is collected by the sFlow agent, you have to define two variables, one of which is optional. The variables are listed here:

❒ Sampling rate (optional)

❒ Polling rate (required)

> **Note**
> If the sFlow agent is already enabled on the switch, it will be necessary to disable it while you set these parameters. For instructions, refer to "Disabling the sFlow Agent" on page 1032.

Configuring the Sampling Rate

If you want the sFlow agent to collect packet samples from the ports on the switch and to send the samples to the sFlow collector, you have to specify sampling rates. The sampling rates define the average number of ingress packets from which one packet is sampled. Each port can have just one sampling rate, but different ports can have different rates. The packet sampling rate is controlled with the SFLOW SAMPLING-RATE command in the Port Interface mode. Here is the format of the command:

```
sflow sampling-rate value
```

The VALUE parameter specifies the average number of ingress packets on a port from which one sample is taken by the agent and sent to the sFlow collector. The permitted values are 0 and 256 to 16441700 packets. For example, if you specify a sampling rate of 10000 packets on a port, the agent samples an average of one packet in 10,000 ingress packets. To disable packet sampling on a port, enter the value 0 for the sampling rate or use the NO form of the command.

This example sets the sampling rate on ports 2 and 3 to 1 packet in every 2000 ingress packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2,port1.0.3
awplus(config-if)# sflow sampling-rate 2000
```

This example disables packet sampling on port 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# no sflow sampling-rate
```

Configuring the Polling Interval

The polling interval determines how frequently the agent queries the packet counters of the ports and sends the data to the collector. This is the maximum amount of time allowed between successive queries of the counters by the agent on the switch. The range is 0 to 16777215 seconds. For example, if you set the polling interval to 400 seconds on a port, the agent polls the counters of the designated port and sends the data to the collector at least once every 400 seconds.

Just as with the sampling rate, a port can have just one polling rate, but different ports can have different settings.

The command to set this value is the SFLOW POLLING-INTERVAL command in the Port Interface mode. Here is the format of the command:

```
sflow polling-interval value
```

This example of the command sets the polling interval to 100 seconds on ports 4, 9, and 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.9,port1.0.11
awplus(config-if)# sflow polling-interval 100
```

To disable the polling of the packet counters on a port, enter the value 0 for the polling interval or use the NO form of this command, as shown in this example, which disables packet counters polling on port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no sflow polling-interval
```

Enabling the sFlow Agent

Use the SFLOW ENABLE command in the Global Configuration mode to activate the sFlow agent so that the switch begins to gather packet samples and packet counters and to transmit the data to the sFlow collector on your network. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# sflow enable
```

This command assumes that you have already performed these steps:

❒ Added the IP address of the collector to the sFlow agent with the SFLOW COLLECTOR IP command.

❒ Used the SFLOW SAMPLING-RATE and SFLOW POLLING-INTERVAL IP commands to configure those ports from which performance data is to be gathered.

❒ Assigned the switch a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

The switch immediately begins transmitting the packet samples and packet counters to the collector as soon as you enter the command.

Disabling the sFlow Agent

To stop the sFlow agent from collecting performance data on the ports on the switch and from sending the data to the collector on your network, use the NO SFLOW ENABLE command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no sflow enable
```

Displaying the sFlow Agent

To view the IP addresses and UDP port settings of the collectors as defined in the sFlow agent on the switch, use the SHOW SFLOW command in the Global Configuration mode. Here is the command:

awplus(config)# show sflow

Here is an example of the display.

```
Number of Collectors: 1
Collector_address      UDP_port
==================     ========
149.122.78.12          6343

Number of Samplers/Pollers 4
Port     Sample-rate        Polling-interval
====     ===========        ================
1.0.4    1000               60
1.0.12   1000               60
1.0.13   50000              2400
1.0.14   50000              2400

   sFlow Status
   ============
   Enabled
```

Figure 174. SHOW SFLOW Command

The fields are described in Table 93 on page 1047.

Configuration Example

Here is an example of how to configure the sFlow agent. The IP address of the sFlow collector is 152.232.56.11. The ports from which performance data will be collected will be ports 3, 11, 12, and 21 to 23. Ports 3, 11,and 12 will have a polling rate of 120 seconds and sampling rate of 1 packet in an average of 10.000 packets. Ports 21 to 23 will have a polling rate of 1800 seconds and sampling rate of 1 packet in every 50.000 packets.

This first series of commands adds the IP address of the sFlow collector to the agent on the switch. You must add the IP address of the collector before configuring the polling and sampling rates of the ports.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# sflow collector ip 152.232.56.11 port 6342`	Use the SFLOW COLLECTOR IP command to add the IP address of the sFlow collector to the sFlow agent on the switch.
`awplus(config)# show sflow`	Use the SHOW SFLOW command to confirm the IP address.

The next series of commands configures the sFlow settings of the ports.

`awplus(config)# interface port1.0.3,port1.0.11, port1.0.12`	From the Global Configuration mode, use the INTERFACE PORT command to enter the Interface mode for ports 3, 11, and 12.
`awplus(config-if)# sflow sampling-rate 10000`	Use the SFLOW SAMPLING-RATE command to set the sampling rate of the ports to 1 packet for every 10000 packets.
`awplus(config-if)# sflow polling-interval 120`	Use the SFLOW POLLING-INTERVAL command to set the polling rate of the statistics counters of the ports to 120 seconds.
`awplus(config)# interface port1.0.21-port1.0.23`	Use the INTERFACE PORT command to enter the Interface mode for ports 21 to 23.

`awplus(config-if)# sflow sampling-rate 50000`	Use the SFLOW SAMPLING-RATE command to set the sampling rate of the ports to 1 packet for every 50000 packets.
`awplus(config-if)# sflow polling-interval 1800`	Use the SFLOW POLLING-INTERVAL command to set the polling rate of the statistics counters of the ports to 1800 seconds.
`awplus(config-if)# exit`	Return to the Global Configuration mode.
`awplus(config)# show sflow`	Use the SHOW SFLOW command again to confirm the configuration of the ports.

This last command activates the sFlow agent on the switch.

`awplus(config)# sflow enable`	Activate the agent with the SFLOW ENABLE command.

Depending on the amount of traffic on the ports and the values of the sampling rates and polling intervals, there may be long periods of time in which the agent on the switch does not send any information to the collectors. For instance, if there is little or no traffic on port 23 in the example, the agent will wait about 30 minutes (1800 seconds) before sending performance data for that particular port.

1036

Chapter 66

sFlow Agent Commands

The sFlow agent commands are summarized in Table 92 and described in detail within the chapter.

Table 92. sFlow Agent Commands

Command	Mode	Description
"NO SFLOW COLLECTOR IP" on page 1038	Global Configuration	Deletes the IP address of an sFlow collector from the switch.
"NO SFLOW ENABLE" on page 1039	Global Configuration	Disables the sFlow agent on the switch.
"SFLOW COLLECTOR IP" on page 1040	Global Configuration	Adds the IP addresses and UDP ports of sFlow collectors on your network to the sFlow agent on the switch.
"SFLOW ENABLE" on page 1041	Global Configuration	Activates the sFlow agent on the switch.
"SFLOW POLLING-INTERVAL" on page 1042	Port Interface	Sets the polling intervals that control the maximum amount of time permitted between successive pollings of the port packet counters by the sFlow agent.
"SFLOW SAMPLING-RATE" on page 1044	Port Interface	Sets the sampling rates that determine the number of ingress packets from which one sample is taken on a port.
"SHOW SFLOW" on page 1046	Global Configuration	Displays the IP addresses and the UDP ports of the sFlow collectors. Also displays the sampling and polling values for the individual ports.

NO SFLOW COLLECTOR IP

Syntax

```
no sflow collector ip ipaddress
```

Parameters

ipaddress
Specifies the IP address of an sFlow collector.

Mode

Global Configuration mode

Description

Use this command to delete the IP address of an sFlow collector from the switch.

Confirmation Command

"SHOW SFLOW" on page 1046

Example

This example deletes the IP address 152.42.175.22 as an sFlow collector from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no sflow collector ip 152.42.175.22
```

NO SFLOW ENABLE

Syntax

```
no sflow enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the sFlow agent to stop the switch from transmitting sample and counter data to the sFlow collector on your network.

Confirmation Command

"SHOW SFLOW" on page 1046

Example

This example disables the sFlow agent:

```
awplus> enable
awplus# configure terminal
awplus(config)# no sflow enable
```

SFLOW COLLECTOR IP

Syntax

```
sflow collector ip ipaddress [port udp_port]
```

Parameters

ipaddress
Specifies the IP address of the sFlow collector on your network.

udp_port
Specifies the UDP port number of the sFlow collector. The default is UDP port 6343.

Mode

Global Configuration mode

Description

Use this command to specify the IP address and UDP port of an sFlow collector on your network. The packet sampling data and the packet counters from the ports are sent by the switch to the specified collector. You can specify just one collector.

If the IP address of a collector has already been assigned to the switch, and you want to change it, you must first delete it using the NO version of this command.

Confirmation Command

"SHOW SFLOW" on page 1046

Example

This example enters the IP address of the collector as 149.112.14.152 and the UDP port as 5622:

```
awplus> enable
awplus# configure terminal
awplus(config)# sflow collector ip 149.112.14.152 port 5622
```

SFLOW ENABLE

Syntax

```
sflow enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the sFlow agent on the switch. The switch uses the agent to gather packet sampling data and packet counters from the designated ports and to transmit the data to the sFlow collector on your network.

Confirmation Command

"SHOW SFLOW" on page 1046

Example

The following example actives the sFlow agent on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# sflow enable
```

SFLOW POLLING-INTERVAL

Syntax

```
sflow polling-interval polling-interval
```

Parameters

polling-interval

Specifies the maximum amount of time permitted between successive pollings of the packet counters of a port by the agent. The range is 0 to 16777215 seconds.

Mode

Port Interface mode

Description

Use this command to set the polling intervals for the ports. This controls the maximum amount of time permitted between successive pollings of the packet counters on the ports by the sFlow agent. The ports can have different polling intervals.

To remove sFlow monitoring from a port, enter the NO form of this command, NO SFLOW POLLING-INTERVAL.

You must disable the sFlow agent to set or change the polling interval of a port. For instructions, refer to "NO SFLOW ENABLE" on page 1039.

Confirmation Commands

"SHOW SFLOW" on page 1046

Examples

This example sets the polling interval for ports 13 to 15 to 3600 seconds (one hour):

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.13-port1.0.15
awplus(config-if)# sflow polling-interval 3600
```

This example removes sFlow monitoring on port 21 using the NO form of the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config-if)# no sflow polling-interval
```

SFLOW SAMPLING-RATE

Syntax

```
sflow sampling-rate sampling-rate
```

Parameters

sampling-rate
> Specifies the sampling rate on a port. The possible values are 0 and 256 to 16441700 packets. The value 0 means no sampling.

Mode

Port Interface mode

Description

Use this command to enable or disable packet sampling on the ports and to set the sampling rates. The sampling rate dictates the number of ingress packets from which one sample is taken on a port and sent by the agent to the sFlow collector. For example, a sample rate of 700 on a port means that one sample packet is taken for every 700 ingress packets. The ports can have different sampling rates.

To disable packet sampling on the ports, enter the value 0 for the sampling rate or use the NO form of this command, NO SFLOW SAMPLING-RATE.

You must disable the sFlow agent to set or change the sampling rate of a port. For instructions, refer to "NO SFLOW ENABLE" on page 1039.

Confirmation Commands

"SHOW SFLOW" on page 1046

Examples

This example configures ports 4 to 8 to sample 1 packet in every 350 ingress packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4-port1.0.8
awplus(config-if)# sflow sampling-rate 350
```

This example disables packet sampling on port 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# no sflow sampling-rate
```

SHOW SFLOW

Syntax

```
show sflow [database]
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the settings of the sFlow agent on the switch. The command displays the same information with or without the DATABASE keyword. Here is an example of the information.

```
Number of Collectors: 1
Collector_address      UDP_port
==================     ========
149.122.78.12          6343

Number of Samplers/Pollers 4
Port      Sample-rate        Polling-interval
====      ===========        ================
1.0.4     1000               60
1.0.12    1000               60
1.0.13    50000              2400
1.0.14    50000              2400

   sFlow Status
   ============
   Enable
```
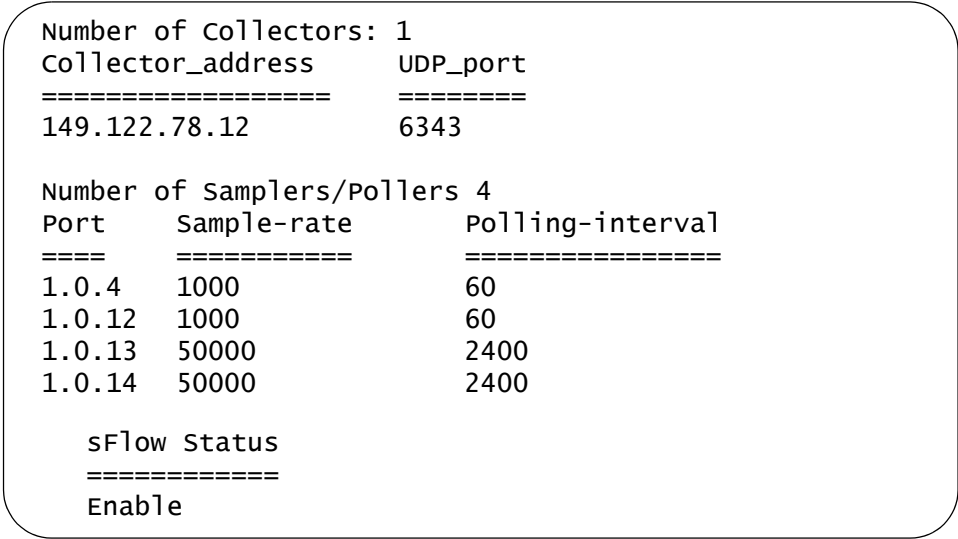
Figure 175. SHOW SFLOW Command

The fields are described in Table 93.

Table 93. SHOW SFLOW Command

Parameter	Description
Number of Collectors	Number of sFlow collectors that have been defined on the switch by having their IP addresses entered in the agent. The agent can contain up to four IP addresses of sFlow collectors.
Collector_address	The IP address of the sFlow collector on your network. To set this parameter, refer to "SFLOW COLLECTOR IP" on page 1040.
UDP_port	The UDP ports of the sFlow collectors. To set this parameter, refer to "SFLOW COLLECTOR IP" on page 1040.
Number of Samplers/ Pollers	Number of ports configured to be sampled or polled.
Port	The port number.
Sample-rate	The rate of ingress packet sampling on the port. For example, a rate of 500 means that one in every 500 packets is sent to the designated collector. A value of 0 means the agent is not sampling packets on the port. To set this value, refer to "SFLOW SAMPLING-RATE" on page 1044.
Polling-interval	The maximum amount of time (seconds) permitted between successive pollings of the packet counters of the port. To set this value, refer to "SFLOW POLLING-INTERVAL" on page 1042.
sFlow Status	The status of the sFlow agent. If the status is enabled, the switch is sending port performance data to the designated collector. If the status is disabled, the switch is not sending performance data. To enable or disable the agent, refer to "SFLOW ENABLE" on page 1041 and "NO SFLOW ENABLE" on page 1039.

Example

This example displays the settings of the sFlow agent:

```
awplus> enable
awplus# show sflow
```

Chapter 67

LLDP and LLDP-MED

This chapter contains the following topics

Overview

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) allow Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. The data sent and received by LLDP and LLDP-MED are useful for many reasons. The switch can discover other devices directly connected to it. Neighboring devices can use LLDP to advertise some parts of their Layer 2 configuration to each other, enabling some kinds of misconfiguration to be more easily detected and corrected.

LLDP is a "one-hop" protocol; LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called neighbors. Advertised information is not forwarded on to other devices on the network. LLDP is a one-way protocol. That is, 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 acknowledgements. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves. In addition, LLDP can be configured on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information 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.

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 TLVs are grouped as follows

❐ "Mandatory LLDP TLVs" on page 1051
❐ "Optional LLDP TLVs" on page 1051
❐ "Optional LLDP-MED TLVs" on page 1053

Mandatory LLDP TLVs

Mandatory LLDP TLVs are sent by default on ports that send TLVs. The TLVs are defined in Table 94.

Table 94. Mandatory LLDP TLVs

TLV	Description
Chassis ID	The device's chassis ID number. For Allied Telesis devices, this is the MAC address of the switch.
Port ID	The number of the port that transmitted the advertisements.
Time to Live (TTL)	The length of time in seconds for which the information received in the advertisements remains valid. If the value is greater than zero, the information is stored in the switch's neighbor table. If the value is zero, the information is no longer valid and is removed from the table.

Optional LLDP TLVs

You can configure the switch to send optional LLDP TLVs along with the mandatory TLVs in the LLDPDUs. The following table describes the optional TLVs from the basic management set and the organizationally specific TLVs from the IEEE 802.1AB TLV set (Annex F).

Table 95. Optional LLDP TLVs

TLV	Description
Port description	A port's description. To add a port description, refer to "Adding Descriptions" on page 172 or "DESCRIPTION" on page 198.
System name	The name of the switch. To assign a name, refer to "Adding a Name to the Switch" on page 114 or "HOSTNAME" on page 145.
System description	A description of the device. This may include information about the device hardware and operating system. The AT-9000 Switch sends its model name as its system description.

Table 95. Optional LLDP TLVs (Continued)

TLV	Description
System capabilities	The device's router and bridge functions, and whether or not these functions are currently enabled. The value for this TLV on the AT-9000 Switch is Bridge, Router.
Management address	The address of the local LLDP agent. This can be used to obtain information related to the local device.
Port VLAN	The VID of the VLAN in which the transmitting port is an untagged member.
Port and protocol VLANs	Whether the device supports protocol VLANs and, if it does, the protocol VLAN identifiers.
VLAN names	The names of the VLANs in which the transmitting port is either an untagged or tagged member.
Protocol IDs	List of protocols that are accessible through the port, for instance: ❐ 9000 (Loopback) ❐ 0026424203000000 (STP, RSTP, or MSTP) ❐ 888e01 (802.1x) ❐ AAAA03 (EPSR) ❐ 88090101 (LACP) ❐ 00540000e302 (Loop protection) ❐ 0800 (IPv4) ❐ 0806 (ARP) ❐ 86dd (IPv6)
MC/PHY Configuration	The speed and duplex mode of the port and whether the port was configured with Auto-Negotiation.
Power management	The power via MDI capabilities of the port.
Link aggregation	Whether the port is capable of link aggregation and, if so, whether it is currently a member of an aggregator.
Maximum frame size	The maximum frame size the port can forward.

The switch does not verify whether a device connected to a port is LLDP-compatible prior to sending mandatory and optional LLDPs.

Optional LLDP-MED TLVs

LLDP-MED is an extension of LLDP that is used between LAN network connectivity devices, such as this switch, and media endpoint devices connected to them, such as IP phones.

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.

LLDP-MED TLVs, unlike the other TLVs, are only sent if the switch detects that an LLDP-MED activated device is connected to a port. Otherwise, LLDP-MED TLVs are not transmitted.

> **Note**
> The switch is not an LLDP-MED activated device. The switch, while capable of transmitting LLDP-MED TLVs to other devices, cannot provide LLDP-MED information about itself.

The LLDP-MED TLVs are listed in Table 96.

Table 96. Optional LLDP-MED TLVs

TLV	Description
Capabilities	The LLDP-MED TLVs that are supported and enabled on the switch, and the device type, which for this switch is Network Connectivity Device.
Network policy	The 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 Class of Service (CoS) priority ❑ Voice VLAN Diffserv Code Point (DSCP)
Location	Location information configured for the port, in one or more of the following formats: ❑ Civic location ❑ Coordinate location ❑ Emergency Location Identification Number (ELIN)

Table 96. Optional LLDP-MED TLVs (Continued)

TLV	Description
Extended power management	The following PoE information: ❒ 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 a 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.
Inventory management	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

Enabling LLDP and LLDP-MED on the Switch

To enable LLDP and LLDP-MED on the switch, use the LLDP RUN command in the Global Configuration mode. The switch begins to transmit advertisements from those ports that are configured to send TLVs, and begins to populate its neighbor information table as advertisements from the neighbors arrive on the ports. The command does not support any parameters. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp run
```

To deactivate LLDP and LLDP-MED, refer to "Disabling LLDP and LLDP-MED on the Switch" on page 1074.

Configuring Ports to Only Receive LLDP and LLDP-MED TLVs

This is the first in a series of examples that show how to configure the ports for LLDP and LLDP-MED. In this first example, ports 4 and 18 are configured to accept advertisements from their neighbors, but not to send any advertisements.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.4,port1.0.18`	Enter the Port Interface mode for ports 4 and 18.
`awplus(config-if)# lldp receive`	Configure the ports to accept TLVs from their neighbors.
`awplus(config-if)# no lldp transmit`	Configure the ports not to send any TLVs.
`awplus(config-if)# end`	Return to the Privileged Exec Mode.
`awplus# show lldp interface port1.0.4,port1.0.18`	Use the SHOW LLDP INTERFACE command to confirm the configuration.

If LLDP is active on the switch, the switch begins to populate the neighbor table as TLVs arrive on ports 4 and 18. The neighbors on those ports do not receive any advertisements from the switch because the ports do not send any TLVs.

Configuring Ports to Send Only Mandatory LLDP TLVs

This example illustrates how to configure the ports to receive and send only the mandatory LLDP TLVs. Since the default is for ports to send all mandatory and optional TLVs, you must remove the optional TLVs. This example configures port 16 to 20:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.16-port1.0.20`	Enter the Port Interface mode for ports 16 to 20.
`awplus(config-if)# lldp transmit receive`	Configure the ports to accept and send TLVs to their neighbors.
`awplus(config-if)# no lldp tlv-select all`	Remove all optional LLDP TLVs with the NO LLDP TLV-SELECT command.
`awplus(config-if)# no lldp med-tlv-select all`	Remove all optional LLDP-MED TLVs with the NO LLDP MED-TLV-SELECT command.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show lldp interface port1.0.16-port1.0.20`	Use the SHOW LLDP INTERFACE command to confirm the configuration.

The ports send only the mandatory LLDP TLVs because no optional TLVs are specified.

Configuring Ports to Send Optional LLDP TLVs

This example illustrates how to configure the ports to send optional LLDP TLVs along with the mandatory TLVs, to their neighbors. Refer to Table 97 for the list of optional LLDP TLVs with brief descriptions. For full descriptions, refer to Table 95 on page 1051.

Table 97. Optional LLDP TLVs - Summary

TLV Designator	Description
port-description	Port description
system-name	System name
system-description	System description
system-capabilities	System capabilities
management-address	Management IP address
port-vlan	Port VLAN
port-and-protocol-vlan	Port and Protocol VLANs
vlan-names	Names of VLANs in which the port is a member.
protocol-ids	Protocol IDs
mac-phy-config	Speed and duplex mode
power-management	Power via MDI capabilities
link-aggregation	Link aggregation status
max-frame-size	The maximum supported frame size of the port.

This example configures ports 18 and 24 to send these optional TLVs, along with the mandatory TLVs:

   ❑ port-description

   ❑ link-aggregation

   ❑ mac-phy-config

Here are the commands to configure the ports to send the TLVs:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.18,port1.0.24`	Enter the Port Interface mode for ports 18 and 24.
`awplus(config-if)# lldp transmit receive`	Configure the ports to accept and send TLVs to and from their neighbors.
`awplus(config-if)# no lldp tlv-select all`	Remove all optional LLDP TLVs from the ports with the NO LLDP TLV-SELECT command.
`awplus(config-if)# no lldp med-tlv-select all`	Remove all optional LLDP-MED TLVs from the ports with the NO LLDP MED-TLV-SELECT command.

`awplus(config-if)# lldp tlv-select port-description`
`awplus(config-if)# lldp tlv-select link-aggregation`
`awplus(config-if)# lldp tlv-select mac-phy-config`
	Add the optional TLVs you want the ports to transmit, with the LLDP TLV-SELECT command.

`awplus(config-if)# end`	Return to the Privileged Exec Mode.
`awplus# show lldp interface port1.0.18,port1.0.24`	Use the SHOW LLDP INTERFACE command to confirm the configuration.

Configuring Ports to Send Optional LLDP-MED TLVs

This section explains how to configure the ports to send these optional LLDP-MED TLVs:

❒ Capabilities

❒ Network-policy

For instructions on how to create LLDP-MED civic, coordinate, and ELIN location entries, refer to the following sections.

The command to configure ports to send the capabilities, network-policy, and inventory-management TLVs is the LLD MED-TLV-SELECT command, which has this format:

`lldp med-tlv-select all|`*`tlv`*

In this example of the command, ports 3 and 4 are configured to send the capabilities and network-policy TLVs:

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.3,port1.0.4`	Enter the Port Interface mode for ports 3 and 4.
`awplus(config-if)# lldp transmit receive`	Configure the ports to accept and send TLVs to and from their neighbors.
`awplus(config-if)# no lldp tlv-select all`	Remove all optional LLDP TLVs from the ports with the NO LLDP TLV-SELECT command.
`awplus(config-if)# no lldp med-tlv-select all`	Remove all optional LLDP-MED TLVs from the ports with the NO LLDP MED-TLV-SELECT command.
`awplus(config-if)# lldp med-tlv-select capabilities` `awplus(config-if)# lldp tlv-select network-policy`	Configure the ports to transmit the capabilities and network-policy TLVs, with the LLDP MED-TLV-SELECT command.
`awplus(config-if)# end`	Return to the Privileged Exec Mode.

awplus# show lldp interface port1.0.3,port1.0.4	Use the SHOW LLDP INTERFACE command to confirm the configuration.

Configuring Ports to Send LLDP-MED Civic Location TLVs

Civic location TLVs specify the physical addresses of network devices. Country, state, street, and building number are only a few examples of the various types of information civic location TLVs can include.

Unlike some of the other LLDP-MED TLVs, such as the capabilities and network policy TLVs, which have pre-set values that you cannot change, a civic location TLV has to be configured before a port will send it. You have to create an entry with the relevant location information, apply it to one or more ports on the switch, and then configure the ports to send it as their civic location TLV.

Here are the main steps to creating civic location TLVs:

1. Starting in the Global Configuration mode, use the LOCATION CIVIC-LOCATION command to assign an ID number to the new Civic Location entry. The command moves you to the Civic mode.

2. Use the parameters in the Civic mode to configure the settings of the entry. An abbreviated list of the parameters is shown in Table 98. For the complete list, refer to Table 102 on page 1105.

Table 98. Abbreviated List of LLDP-MED Civic Location Entry Parameters

Parameter	Example
building	102
city	San-Jose
country	US
county	Santa-Clara
division	North-Brookview
floor	4
house-number	401
house-number-suffix	C
name	J-Smith
post-office-box	102
postal-code	95134
primary-road-name	Eastwood
room	402

Table 98. Abbreviated List of LLDP-MED Civic Location Entry Parameters

Parameter	Example
seat	cube-411a
state	CA
street-suffix	Blvd
unit	A11

3. Move to the Port Interface mode of the ports to which the entry is to be assigned. (A civic location entry can be applied to more than one port.)

4. Use the LLDP LOCATION command in the Port Interface mode to attach the location entry to the port.

5. Use the LLDP MED-TLV-SELECT command in the Port Interface mode to configure the ports to send the TLV in their advertisements.

This example creates a civic location entry for port 14. The address information of the entry, which is assigned the ID number 8, is listed here:

1020 North Hacienda Avenue
San Jose, CA 95132

This first series of commands creates the location entry.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# location civic-location identifier 8`	Use the LOCATION CIVIC-LOCATION command to assign an ID number in the range of 1 to 256 to the entry and to enter the Civic mode. This example assigns the entry the ID number 8.

`awplus(config_civic)# country US`
`awplus(config_civic)# state CA`
`awplus(config_civic)# city San-Jose`
`awplus(config_civic)# building 1020`
`awplus(config_civic)# primary-road-name North-Hacienda`
`awplus(config_civic)# street-suffix Avenue`
`awplus(config_civic)# postal-code 95132`
	Use the appropriate parameter commands to define the entry.

`awplus(config_civic)# exit`	Return to the Global Configuration mode.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show location civic-location identifier 8`	Use the SHOW LOCATION command to verify the configuration of the new location entry.

This series of commands adds the new location entry to port 14 and configures the port to include the location TLV in its advertisements:

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.14`	Enter the Port Interface mode for port 14.
`awplus(config-if)# lldp transmit receive`	Configure the port to send and receive LLDP advertisements.
`awplus(config-if)# lldp location civic-location-id 8`	Use the LLDP LOCATION command to add the civic location entry, ID number 8, to the port.
`awplus(config-if)# lldp med-tlv-select location`	Use the LLDP MED-TLV-SELECT command to configure the port to send the location TLV in its advertisements.
`awplus(config-if)# end`	Return to the Privileged Exec Mode.
`awplus# show location civic-location interface port1.0.14`	Use the SHOW LOCATION command to confirm the assignment of the civic location entry to the port.
`awplus# show lldp interface port1.0.14`	Use the SHOW LLDP INTERFACE command to confirm the port is configured to send the location entry.

Configuring Ports to Send LLDP-MED Coordinate Location TLVs

Coordinate location TLVs specify the locations of network devices by their latitudes and longitudes. Here are the main steps to creating coordinate location TLVs:

1. Starting from the Global Configuration mode, use the LOCATION COORD-LOCATION command to assign the new entry an ID number. The command automatically takes you to the Coordinate mode.

2. Use the parameter commands in the Coordinate mode to configure the new entry. The parameters are listed in Table 99.

Table 99. LLDP-MED Coordinate Location Entry Parameters

Parameter	Value
latitude	Latitude value in decimal degrees. The range is -90.0º to 90.0º. The parameter accepts up to eight digits to the right of the decimal point.
lat-resolution	Latitude resolution as the number of valid bits. The range is 0 to 34.
longitude	Longitude value in decimal degrees. The range is -180.0º to 180.0º. The parameter accepts up to eight digits to the right of the decimal point.
long-resolution	Longitude resolution as number of valid bits. The range is 0 to 34 bits.
altitude floors	Altitude in number of floors. The range is -2097151.0 to 2097151.0. The value for this parameter must be specified between the two keywords, as shown here: altitude *n* floors
altitude meters	Altitude in meters. The range is -2097151.0 to 2097151.0. The parameter accepts up to eight digits to the right of the decimal point. The value for this parameter must be specified between the two keywords, as shown here: altitude *n* meters

Table 99. LLDP-MED Coordinate Location Entry Parameters

Parameter	Value
alt-resolution	Altitude resolution as number of valid bits. The range is 0 to 30 bits.
datum nad83-mllw|nad83-navd| wgs84	The geodetic system (or datum) of the coordinates. The selections are: ❐ nad83-mllw - Mean lower low water datum 1983 ❐ nad83-navd - North American vertical datum 1983 ❐ wgs84 - World Geodetic System 1984

3. Move to the Port Interface mode of the ports to which the entry is to be assigned. (A coordinate location entry can be applied to more than one port.)

4. Use the LLDP LOCATION command in the Port Interface mode to attach the location entry to the ports.

5. Use the LLDP MED-TLV-SELECT command in the Port Interface mode to configure the ports to send the TLV in their advertisements.

Here is an example of how to create a coordinate location entry and apply it to a port. The specifications of the entry are:

```
ID number:    16
Latitude:     37.29153547
Longitude:    --121.91528320
Datum:        nad83-navd
Altitude:     10.25 meters
```

The example is assigned to port 15.

The first series of commands creates the coordinate location entry.

awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.

awplus(config)# location coord-location identifier 16	Use the LOCATION COORD-LOCATION command to assign an ID number in the range of 1 to 256 to the new location entry, and to enter the Coordinate mode. The entry in this example is assigned the ID number 16.
awplus(config_coord)# latitude 37.29153547 awplus(config-coord)# lat-resolution 12 awplus(config_coord)# longitude -121.91528320 awplus(config-coord)# long-resolution 33 awplus(config_coord)# datum nad83-navd awplus(config_coord)# altitude 10.25 meters awplus(config-coord)# alt-resolution 23	Use the parameter commands to define the entry.
awplus(config_coord)# exit	Return to the Global Configuration mode.
awplus(config) exit	Return to the Privileged Exec mode.
awplus# show location coord-location identifier 16	Confirm the configuration of the new coordinate location entry with the SHOW LOCATION command.

This series of commands adds the entry to port 15 and configures the port to include the TLV in its advertisements:

awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface port1.0.15	Enter the Port Interface mode for port 15.
awplus(config-if)# lldp transmit receive	Configure the port to send and receive LLDP advertisements.
awplus(config-if)# lldp location coord-location-id 16	Use the LLDP LOCATION command to add the coordinate location entry, ID number 16, to the port.
awplus(config-if)# lldp med-tlv-select location	Use the LLDP MED-TLV-SELECT command to configure the port to send the location entry in its advertisements.
awplus(config-if)# end	Return to the Privileged Exec mode.

```awplus# show location coord-location interface port1.0.15```
 	
```ID   Element Type   Element Value```
```---```
```16   Latitude Resolution 12 bits```
```   Latitude   37.29153547 degrees```
```   Longitude Resolution 33 bits```
```   Longitude   121.9152832 degrees```
```   Altitude Resolution 23 bits```
```   Altitude   10.25000000 meters```
```   Map Datum   NAD83-NAVD```
	Use the SHOW LOCATION command to confirm the configuration.

```awplus# show lldp interface port1.0.15```	Use the SHOW LLDP INTERFACE command to confirm the port is configured to send the location entry.

1068

Configuring Ports to Send LLDP-MED ELIN Location TLVs

This type of TLV specifies the location of a network device by its ELIN (emergency location identifier number). Here are the main steps to creating ELIN location TLVs:

1. Starting from the Global Configuration mode, use the LOCATION ELIN-LOCATION command to create the new entry.

2. In the Port Interface mode, use the LLDP LOCATION command to add the entry to the appropriate ports. (An ELI location entry can be applied to more than one port.)

3. In the Port Interface mode, use the LLDP MED-TLV-SELECT command to configure the ports to send the TLV in their advertisements.

Here is an example of how to create an ELIN location entry and apply it to a port. The specifications of the entry are:

ID number: 3
ELIN: 1234567890

The example is assigned to port 5.

The first series of commands creates the coordinate location entry.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# location elin-location 1234567890 identifier 3`	Use the LOCATION ELIN-LOCATION command to create the entry.
`awplus(config) exit`	Return to the Privileged Exec mode.
`awplus# show location elin-location identifier 3`	Confirm the configuration of the new ELIN location entry with the SHOW LOCATION command.

This series of commands adds the entry to port 5 and configures the port to include the TLV in its advertisements:

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.5`	Enter the Port Interface mode for port 5.
`awplus(config-if)# lldp transmit receive`	Configure the port to send and receive LLDP advertisements.
`awplus(config-if)# lldp location elin-location-id 3`	Use the LLDP LOCATION command to add the ELIN location entry, ID number 3, to the port.
`awplus(config-if)# lldp med-tlv-select location`	Use the LLDP MED-TLV-SELECT command to configure the port to send the location entry in its advertisements.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show location elin-location interface port1.0.5`	Use the SHOW LOCATION command to confirm the configuration.
`awplus# show lldp interface port1.0.5`	Use the SHOW LLDP INTERFACE command to confirm the port is configured to send the location entry.

Removing LLDP TLVs from Ports

To stop ports from sending optional LLDP TLVs, use this command:

```
no lldp tlv-select all|tlv
```

The command is located in the Port Interface mode. You can specify only one TLV at a time in the command. This example stops ports 4 and 5 from including the system capabilities and the management address TLVs in their advertisements:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.5
awplus(config-if)# no lldp tlv-select system-capabilities
awplus(config-if)# no lldp tlv-select management-address
```

This example stops port 8 from transmitting all optional LLDP TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# no lldp tlv-select all
```

Removing LLDP-MED TLVs from Ports

To remove optional LLDP-MED TLVs from ports, use the NO LLDP MED-TLV-SELECT command:

```
no lldp med-tlv-select capabilities|network-
policy|location|power-management-ext|inventory-
management|all
```

You can specify only one TLV at a time in the command, which is located in the Port Interface mode. This example stops ports 6 and 11 from sending the location and inventory management TLVs in their advertisements:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6,port1.0.11
awplus(config-if)# no lldp med-tlv-select location
awplus(config-if)# no lldp med-tlv-select inventory-
management
```

This example stops port 15 from transmitting all optional LLDP-MED TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# no lldp med-tlv-select all
```

1072

Deleting LLDP-MED Location Entries

The command for deleting LLDP-MED location entries from the switch is:

```
no location civic-location|coord-location|elin-location
identifier id_number
```

The command, which is located in the Global Configuration mode, can delete only one entry at a time and must include both the type and the ID number of the location entry to be deleted.

This example deletes the civic location ID 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# no location civic-location-id 22
```

This example deletes the coordinate location ID 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# no location coord-location-id 8
```

This example deletes the ELIN location ID 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# no location elin-location-id 3
```

Disabling LLDP and LLDP-MED on the Switch

To disable LLDP and LLDP-MED on the switch, use the NO LLDP RUN command in the Global Configuration mode. The command has no parameters. After the protocols are disabled, the switch neither sends advertisements to nor collects information from its neighbors. The switch retains its LLDP settings. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no lldp run
```

Displaying General LLDP Settings

To view the timers and other general LLDP and LLDP-MED settings, use the SHOW LLDP command in the User Exec mode or the Privileged Exec mode. Here is the command:

```
awplus# show lldp
```

Here is an example of the information.

```
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]
Fast Start Count.......... 3 [3]

LLDP Global Status:
Total Neighbor Count ...... 47
Neighbors table last updated 0 hrs 0 mins 43 secs ago
```

Figure 176. SHOW LLDP Command

The fields are defined in Table 104 on page 1121.

Displaying Port Settings

To view the LLDP and LLDP-MED settings of the individual ports on the switch, use the SHOW LLDP INTERFACE command. The command has this format:

show lldp interface [*port*]

If you omit the PORT variable, as in this example, the command displays the settings for all the ports.

awplus# show lldp interface

This example displays the settings for ports 17 and 19:

show lldp interface port1.0.17,port1.0.19

Here is an example of the information.

```
LLDP Port Status and Configuration:
  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    Rx Tx  -- --  0.0.0.0         PdSmSdSc-- Pv--VnPi MpPoLaMf McNpLo--In
 2    Rx Tx  -- --  0.0.0.0         PdSmSdSc-- Pv--VnPi MpPoLaMf McNpLo--In
 3    Rx --  -- --  0.0.0.0         ---------- -------- -------- ----------
 4    Rx Tx  -- --  149.124.36.15   PdSmSdScMa Pv--VnPi MpPoLaMf McNpLo--In
 5    Rx Tx  -- --  149.124.36.15   PdSmSdScMa Pv--VnPi MpPoLaMf McNpLo--In
```

Figure 177. SHOW LLDP INTERFACE Command

Displaying or Clearing Neighbor Information

There are two commands for displaying the information the switch has collected from the LLDP and LLDP-MED-compatible neighbors connected to its ports. To view a summary of the information, use the SHOW LLDP NEIGHBORS command in the User Exec mode or the Privileged Exec mode. The command has this format:

```
show lldp neighbors [interface port]
```

This example displays summary information for all the neighbors on the switch:

```
awplus# show lldp neighbors
```

This example displays summary information for the neighbors connected to ports 2 and 3:

```
awplus# show lldp neighbors interface port1.0.2,port1.0.3
```

Here is an example of the summary information:

The fields are defined in Table 106 on page 1132.

To view all the neighbor information, use the SHOW LLDP NEIGHBORS DETAIL command. The command has this format:

```
show lldp neighbors detail [interface port]
```

This example displays detailed information about all the neighbors:

```
awplus# show lldp neighbors detail
```

This example displays detailed information about the neighbor connected to port 23:

```
awplus# show lldp neighbors detail interface 23
```

An example of the information is provided in Figure 105 on page 1128 and Figure 106 on page 1132. The fields are defined in Table 105 on page 1128.

When the TTL value for a neighbor's information expires, the switch automatically deletes the information from the table so that the table contains only the most recent information. But if you need to, you can delete information manually with the CLEAR LLDP TABLE command:

```
clear lldp table [interface port]
```

This example clears the information the switch has received from all the neighbors:

```
awplus> enable
awplus# clear lldp table
```

This example clears the information the switch has received from the neighbor connected to port 11:

```
awplus> enable
awplus# clear lldp table interface port1.0.11
```

Displaying Port TLVs

To view the TLVs of the individual ports on the switch, use the SHOW LLDP LOCAL-INFO INTERFACE command in the User Exec mode or the Privileged Exec mode. This command is useful whenever you want to confirm the TLVs on the ports, such as after you have configured the ports or if you believe that ports are not sending the correct information.

The command has this format:

```
show lldp local-info [interface port]
```

To view the TLVs on all the ports, enter this command:

```
awplus# show lldp local-info
```

This example displays the TLVs currently configured on port 2:

```
awplus# show lldp local-info interface port1.0.2
```

Refer to Figure 181 on page 1125 and Figure 182 on page 1126 for an example of the information. The fields are defined in Table 105 on page 1128.

Displaying and Clearing Statistics

The switch maintains LLDP and LLDP-MED performance statistics for the the individual ports and the entire unit. The command to display the statistics for the entire switch is the SHOW LLDP STATISTICS command in the Privileged Exec mode. (The LLDP and LLDP-MED SHOW commands, unlike the SHOW commands for the other features, are not available in the User Exec mode.) Here is the command:

```
awplus# show lldp statistics
```

Here is an example of the information the command displays. The fields are defined in Table 107 on page 1134.

```
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
```

Figure 178. SHOW LLDP STATISTICS Command

To view the same statistics for individual ports, use this command:

```
show lldp statistics interface port
```

You can view the statistics of more than one port at a time, as demonstrated in this example, which displays the LLDP statistics for ports 2 and 3:

```
awplus# show lldp statistics interface port1.0.2,port1.0.3
```

To clear the statistics on the ports, use this command, which, as with the SHOW command, is found in the Privileged Exec mode:

```
clear lldp statistics [interface port]
```

This example clears the statistics for all the ports on the switch:

```
awplus# clear lldp statistics
```

This example clears the statistics for ports 9 and 10:

```
awplus# clear lldp statistics interface port1.0.9,port1.0.10
```

Chapter 68

LLDP and LLDP-MED Commands

The Link Layer Discovery Protocol commands are summarized in Table 100 and described in detail within the chapter.

Table 100. LLDP and LLDP-MED Commands

Command	Mode	Description
"CLEAR LLDP STATISTICS" on page 1084	Privileged Exec	Clears the LLDP statistics (packet and event counters) on the ports.
"CLEAR LLDP TABLE" on page 1085	Privileged Exec	Clears the LLDP information the switch has received from its neighbors.
"LLDP HOLDTIME-MULTIPLIER" on page 1086	Global Configuration	Sets the holdtime multiplier value, which the switch uses to calculate the Time To Live (TTL) that it advertises to the neighbors.
"LLDP LOCATION" on page 1087	Port Interface	Adds LLDP-MED location information to the ports on the switch.
"LLDP MANAGEMENT-ADDRESS" on page 1089	Port Interface	Replaces the default management IP address TLV on the ports.
"LLDP MED-NOTIFICATIONS" on page 1091	Port Interface	Configures the switch to send LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports.
"LLDP MED-TLV-SELECT" on page 1092	Port Interface	Specifies the LLDP-MED TLVs the ports are to transmit to their neighbors.
"LLDP NON-STRICT-MED-TLV-ORDER-CHECK" on page 1094	Global Configuration	Configures the switch to either accept or discard LLDP-MED advertisements if the TLVs are not in standard order.
"LLDP NOTIFICATIONS" on page 1095	Port Interface	Configures ports to send LLDP SNMP notifications (traps).

1081

Table 100. LLDP and LLDP-MED Commands (Continued)

Command	Mode	Description
"LLDP NOTIFICATION-INTERVAL" on page 1096	Global Configuration	Sets the notification interval, which is the minimum interval between LLDP SNMP notifications (traps).
"LLDP REINIT" on page 1097	Global Configuration	Sets the re-initialization delay, which is the number of seconds that must elapse after LLDP is disabled on a port before it can be re-initialized.
"LLDP RUN" on page 1098	Global Configuration	Activates LLDP on the switch.
"LLDP TIMER" on page 1099	Global Configuration	Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements.
"LLDP TLV-SELECT" on page 1100	Port Interface	Specifies the optional LLDP TLVs that the ports transmit to their neighbors.
"LLDP TRANSMIT RECEIVE" on page 1103	Port Interface	Configures ports to transmit to and/or accept LLDP and LLDP-MED advertisements from their neighbors.
"LLDP TX-DELAY" on page 1104	Global Configuration	Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information.
"LOCATION CIVIC-LOCATION" on page 1105	Global Configuration	Creates new LLDP-MED civic location entries and removes parameter values from existing entries.
"LOCATION COORD-LOCATION" on page 1108	Global Configuration	Creates new LLDP-MED coordinate location entries and removes parameter values from existing entries.
"LOCATION ELIN-LOCATION" on page 1111	Global Configuration	Creates new LLDP-MED ELIN location entries and removes parameter values from existing entries.
"NO LLDP MED-NOTIFICATIONS" on page 1112	Port Interface	Configures the switch not to send LLDP-MED topology change notifications when devices are connected to or disconnected from the specified ports.

Table 100. LLDP and LLDP-MED Commands (Continued)

Command	Mode	Description
"NO LLDP MED-TLV-SELECT" on page 1113	Port Interface	Stops ports from transmitting specified LLDP-MED TLVs.
"NO LLDP NOTIFICATIONS" on page 1115	Port Interface	Prevents ports from sending LLDP SNMP notifications (traps).
"NO LLDP RUN" on page 1116	Global Configuration	Disables LLDP on the switch.
"NO LLDP TLV-SELECT" on page 1117	Port Interface	Stops ports from sending optional LLDP TLVs to their neighbors.
"NO LLDP TRANSMIT RECEIVE" on page 1118	Port Interface	Stop ports from transmitting and/or accepting LLDP advertisements.
"NO LOCATION" on page 1119	Port Interface	Removes LLDP-MED location information from the ports on the switch.
"SHOW LLDP" on page 1121	Privileged Exec	Displays general LLDP settings.
"SHOW LLDP INTERFACE" on page 1123	Privileged Exec	Displays the LLDP port settings.
"SHOW LLDP LOCAL-INFO INTERFACE" on page 1125	Privileged Exec	Displays the current configurations of the LLDP advertisements that the ports on the switch can transmit to LLDP-compatible neighbors.
"SHOW LLDP NEIGHBORS DETAIL" on page 1127	Privileged Exec	Displays detailed information the switch has collected from its LLDP-compatible neighbors.
"SHOW LLDP NEIGHBORS INTERFACE" on page 1132	Privileged Exec	Displays a summary of the information gathered by the switch from its LLDP-compatible neighbors.
"SHOW LLDP STATISTICS" on page 1134	Privileged Exec	Displays the LLDP statistics for the entire switch.
"SHOW LLDP STATISTICS INTERFACE" on page 1136	Privileged Exec	Displays the LLDP statistics for the individual ports.
"SHOW LOCATION" on page 1138	Privileged Exec	Displays the civic, coordinate, and ELIN location entries on the switch.

CLEAR LLDP STATISTICS

Syntax

```
clear lldp statistics [interface port]
```

Parameters

port

Specifies a port. You can specify more than one port at a time in this command. Omitting this parameter. specifies all the ports.

Mode

Privileged Exec mode

Description

Use this command to clear the LLDP statistics (packet and event counters) on the ports. You can delete the statistics from all ports or from selected ports.

Examples

This example clears the statistics of all ports:

```
awplus> enable
awplus# clear lldp statistics
```

This example clears the statistics for ports 1 to 3:

```
awplus> enable
awplus# clear lldp statistics port1.0.1-port1.0.3
```

CLEAR LLDP TABLE

Syntax

```
clear lldp table [interface port]
```

Parameters

port

Specifies a port. You can specify more than one port at a time in this command. Omitting this parameter specifies all the ports.

Mode

Privileged Exec mode

Description

Use this command to clear the LLDP and LLDP-MED information the switch has received from its neighbors. You can delete all the information the switch has amassed or only the information from neighbors on selected ports.

Examples

This example clears the information the switch has received from all neighbors:

```
awplus> enable
awplus# clear lldp table
```

This example clears the information the switch has received from the neighbors connected to ports 6 and 8:

```
awplus> enable
awplus# clear lldp table interface port1.0.6,port1.0.8
```

LLDP HOLDTIME-MULTIPLIER

Syntax

```
lldp holdtime-multiplier holdtime-multiplier
```

Parameters

holdtime-multiplier
Specifies the holdtime multiplier value. The range is 2 to 10.

Mode

Global Configuration mode

Description

Use this command to set the holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors. The transmit interval is set with "LLDP TIMER" on page 1099.

Confirmation Command

"SHOW LLDP" on page 1121.

Example

This example sets the holdtime multiplier to 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp holdtime-multiplier 7
```

LLDP LOCATION

Syntax

lldp location *civic-location-id|coord-location-id|elin-location-i*d *location_id*

Parameters

civic-location-id
Adds a civic location to the ports.

coord-location-id
Adds a coordinate location to the ports.

elin-location-idA
dds an ELIN location to the ports.

location-id
Specifies the ID number of the location information to be added to the ports. You can add only one location at a time.

Mode

Port Interface mode

Description

Use this command to add LLDP-MED location information to the ports on the switch. The same command is used to add civic, coordinate and ELIN locations. The specified location entry must already exist.

To remove LLDP-MED location information from the ports, use the NO form of this command. You do not have to specify ID numbers when removing location entries from the ports.

Confirmation Command

"SHOW LOCATION" on page 1138.

Examples

This example adds the civic location ID 5 to ports 3 and 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3,port1.0.4
awplus(config_if)# lldp location civic-location-id 5
```

This example adds the coordinate location ID 11 to port 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config_if)# lldp location coord-location-id 11
```

This example adds the ELIN location ID 27 to port 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21
awplus(config_if)# lldp location elin-location-id 27
```

This example removes the civic location from port 25:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.25
awplus(config_if)# no lldp location civic-location-id
```

LLDP MANAGEMENT-ADDRESS

Syntax

lldp management-address *ipaddress*

Parameters

ipaddress
Specifies an IP address.

Mode

Port Interface mode

Description

Use this command to replace the default management IP address TLV of a port. The management IP address TLV is optional. A port must be configured to transmit it.

A port can have one of two possible default values for the management IP address TLV. The default value depends on whether a port is a member of the same VLAN as the management IP address, if present. Here are the possible default values for a port:

❒ A port that belongs to the same VLAN as the management IP address uses the address as its TLV default value.

❒ A port that belongs to a VLAN that does not have a management IP address, either because no address has been assigned to the switch or it is assigned to a different VLAN, uses the MAC address of the switch as its default value for this TLV.

❒ A port that belongs to more than one VLAN uses the management IP address as its default value if the address is assigned to its lowest numbered VLAN. Otherwise, it uses the switch's MAC address.

To return a port's management IP address TLV to the default value, use the NO form of this command.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Examples

This example configures port 2 to transmit the IP address 149.122.54.2 as its management IP address TLV:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lldp management-address 149.122.54.2
```

This example returns the management IP address TLV on port 18 to its default value:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18
awplus(config-if)# no lldp management-address
```

LLDP MED-NOTIFICATIONS

Syntax

```
lldp med-notifications
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure the switch to send LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports. To prevent the switch from transmitting topology change notifications, refer to "NO LLDP NOTIFICATIONS" on page 1115.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Example

This example configures the switch to send LLDP-MED topology change notifications whenever devices are connected to, or removed from, ports 11 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11,port1.0.17
awplus(config-if)# lldp med-notifications
```

LLDP MED-TLV-SELECT

Syntax

```
lldp med-tlv-select capabilities|network-
policy|location|power-management-ext|inventory-
management|all
```

Parameters

capabilities
> Specifies the capabilities TLV.

network-policy
> Specifies the network policy TLV.

location
> Specifies the location identification TLV.

power-management-ext
> Specifies the extended power-via-MDI TLV.

inventory-management
> Specifies the inventory management TLV.

all
> Configures a port to send all LLDP-MED TLVs.

Mode

Port Interface mode

Description

Use this command to specify the LLDP-MED TLVs the ports are to transmit to their neighbors. The default setting is for the ports to send all the LLDP-MED TLVs, except for the inventory TLV. You can specify only one TLV per command. To remove LLDP-MED TLVs from the ports, refer to "NO LLDP MED-TLV-SELECT" on page 1113.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Examples

This example configures ports 3 to 8 to send the inventory management TLV to their neighbors:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3-port1.0.8
awplus(config-if)# lldp med-tlv-select inventory-management
```

This example configures port 2 to send the capabilities and the location TLVs to its neighbor:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lldp med-tlv-select capabilities
awplus(config-if)# lldp med-tlv-select location
```

LLDP NON-STRICT-MED-TLV-ORDER-CHECK

Syntax

```
lldp non-strict-med-tlv-order-check
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to configure the switch to accept LLDP-MED advertisements even if the TLVs are not in the standard order, as specified in ANSI/TIA-1057. This configuration is useful if the switch is connected to devices that send LLDP-MED advertisements in which the TLVs are not in the standard order.

Use the NO form of this command to configure the switch to accept only advertisements with TLVs that adhere to the correct order. Advertisements in which the TLVs are not in the standard order are discarded by the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example configures the switch to accept LLDP-MED advertisements in which the TLVs are not in standard order:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp non-strict-med-tlv-order-check
```

This example configures the switch to discard LLDP-MED advertisements in which the TLVs are not in standard order:

```
awplus> enable
awplus# configure terminal
awplus(config)# no lldp non-strict-med-tlv-order-check
```

LLDP NOTIFICATIONS

Syntax

```
lldp notifications
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure ports to send LLDP SNMP notifications (traps). To prevent ports from transmitting LLDP SNMP notifications, refer to "NO LLDP NOTIFICATIONS" on page 1115.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Example

This example configures ports 2 and 3 to transmit SNMP notifications:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2,port1.0.3
awplus(config-if)# lldp notifications
```

LLDP NOTIFICATION-INTERVAL

Syntax

```
lldp notification-interval interval
```

Parameters

interval
Specifies the notification interval. The range is 5 to 3600 seconds.

Mode

Global Configuration mode

Description

Use this command to set the notification interval. This is the minimum interval between LLDP SNMP notifications (traps).

Confirmation Command

"SHOW LLDP" on page 1121

Example

This example sets the notification interval to 35 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp notification-interval 35
```

1096

LLDP REINIT

Syntax

```
lldp reinit delay
```

Parameters

delay
> Specifies the re-initialization delay value. The range is 1 to 10 seconds.

Mode

Global Configuration mode

Description

Use this command to set the re-initialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be re-initialized.

Confirmation Command

"SHOW LLDP" on page 1121.

Example

This example set the re-initialization delay to 8 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp reinit 8
```

LLDP RUN

Syntax

```
lldp run
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate LLDP on the switch. Once you have activated LLDP, the switch begins to transmit and accept advertisements on its ports. To deactivate LLDP, refer to "NO LLDP RUN" on page 1116.

Confirmation Command

"SHOW LLDP" on page 1121.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp run
```

LLDP TIMER

Syntax

```
lldp timer interval
```

Parameters

interval
> Specifies the transmit interval. The range is 5 to 32768 seconds.

Mode

Global Configuration mode

Description

Use this command to set the transmit interval. This is the interval between regular transmissions of LLDP advertisements. The transmit interval must be at least four times the transmission delay timer, set with "LLDP TX-DELAY" on page 1104.

Confirmation Command

"SHOW LLDP" on page 1121

Example

This example sets the transmit interval to 60 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp timer 60
```

LLDP TLV-SELECT

Syntax

```
lldp tlv-select all/tlv
```

Parameters

all

> Configures a port to send all optional TLVs.

tlv

> Specifies an optional TLV that a port should transmit to its neighbor. You can specify only one TLV per command.

Mode

Port Interface mode

Description

Use this command to specify the optional LLDP TLVs that ports are to transmit to their neighbors. You can specify only one TLV in a command. To select all the TLVs, use the ALL option. The optional TLVs are listed in Table 101.

Table 101. Optional TLVs

TLV	Description
all	Sends all optional TLVs.
link-aggregation	Advertises link-aggregation values.
mac-phy-config	Identifies MAC and PHY configuration status.
management-address	Sends the management IP address of the port. To set this TLV, refer to "LLDP MANAGEMENT-ADDRESS" on page 1089.
max-frame-size	Sends the maximum supported frame size of the port. This is not adjustable on the switch.
port-and-protocol-vlan	Transmits whether port and protocol VLANs are supported and enabled on the port, and the list of port and protocol VLAN identifiers.

Table 101. Optional TLVs (Continued)

TLV	Description
port-description	Sends a port's description. To configure a port's description, refer to "Adding Descriptions" on page 172 or "DESCRIPTION" on page 198.
port-vlan	Sends the ID number (VID) of the port-based or tagged VLAN where the port is an untagged member.
power-management	Transmits Power over Ethernet (PoE) information.
protocol-ids	Transmits the protocols that are accessible through the port.
system-capabilities	The device's functions, and whether or not these functions are currently enabled.
system-description	Sends the model name of the switch.
system-name	Sends the name of the switch. To assign a name to the switch, refer to "Adding a Name to the Switch" on page 114 or "HOSTNAME" on page 145.
vlan-names	Sends the names of the port-based and tagged VLANs where the port is a member.

To remove optional TLVs from ports, refer to "NO LLDP TLV-SELECT" on page 1117.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Examples

This example configures ports 3 to 5 to transmit all the optional LLDP TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3-port1.0.5
awplus(config-if)# lldp tlv-select all
```

This example configures ports 14 and 22 to transmit the optional LLDP port-description, port-vlan, and system-description TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14,port1.0.22
awplus(config-if)# lldp tlv-select port-description
awplus(config-if)# lldp tlv-select port-vlan
awplus(config-if)# lldp tlv-select system-description
```

1102

LLDP TRANSMIT RECEIVE

Syntax

```
lldp transmit receive/transmit
```

Parameters

transmit
Configures ports to send LLDP advertisements.

receive
Configures ports to accept LLDP advertisements.

Mode

Port Interface mode

Description

Use this command to configure ports to transmit and/or accept LLDP advertisements. Ports configured to transmit LLDP advertisements send the mandatory TLVs and any optional LLDP TLVs they have been configured to send. Ports configured to receive LLDP advertisements accept all advertisements from their neighbors.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123.

Examples

This example configures ports 14 and 22 to both transmit and receive LLDP advertisements:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14,port1.0.22
awplus(config-if)# lldp transmit receive
```

This example configures ports 16 to 22 to only receive LLDP advertisements:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16-port1.0.22
awplus(config-if)# lldp receive
```

LLDP TX-DELAY

Syntax

```
lldp tx-delay tx-delay
```

Parameters

tx-delay
> Specifies the transmission delay timer in seconds. The range is 1 to 8192 seconds.

Mode

Global Configuration mode

Description

Use this command to set the value of the transmission delay timer. This is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The transmission delay timer cannot be greater than a quarter of the transmit interface, set with "LLDP TIMER" on page 1099. To view the current value, refer to "SHOW LLDP" on page 1121.

Confirmation Command

"SHOW LLDP" on page 1121

Example

This example sets the transmission delay timer to 120 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# lldp tx-delay 120
```

LOCATION CIVIC-LOCATION

Syntax

```
location civic-location identifier id_number
```

Parameters

id_number

> Specifies an ID number for an LLDP-MED civic location entry on the switch. The range is 1 to 256. (This range is separate from the ID number ranges for coordinate and ELIN location entries.) You can specify only one ID number.

Mode

Global Configuration mode

Description

Use this command to create or modify LLDP-MED civic location entries on the switch. This command moves you to the Civic Location mode which contains the parameters you use to define or modify an entry. The parameters are listed in Table 102.

Table 102. LLDP-MED Civic Location Entry Parameters

Parameter	Example
additional-code	12345
additional-information	Updated-Aug-2010
branch-road-name	Slate-Lane
building	102
city	San-Jose
country	US
county	Santa-Clara
division	North-Brookview
floor	4
house-number	401
house-number-suffix	C
landmark	city-library

Table 102. LLDP-MED Civic Location Entry Parameters (Continued)

Parameter	Example
leading-street-direction	West
name	J-Smith
neighborhood	Cliffside
place-type	Business-district
post-office-box	102
postal-code	95134
postal-community-name	Lyton
primary-road-name	Eastwood
road-section	North
room	402
seat	cube-411a
state	CA
street-group	Addison
street-name-post-modifier	Div.
street-name-pre-modifier	West
street-suffix	Blvd
sub-branch-road-name	Boulder-Creek-Avenue
trailing-street-suffix	Avenue
unit	A11

Here are the guidelines to using the location parameters:

❐ The country parameter must be two uppercase characters (for example, US).

❐ The other parameters accept uppercase and lowercase characters and have a maximum character length of fifty characters.

❐ Each parameter can have only one value.

❐ The values cannot contain spaces.

❐ You can use as few or as many of the parameters as needed.

❐ You can combine any of the parameters in a single location entry.

❐ To remove parameters from a location entry, use the NO forms of the parameter commands (for example, NO UNIT).

After you create a location entry, use "LLDP LOCATION" on page 1087 to assign the location entry to a port, or ports, on the switch.

To remove a civic location entry, use "NO LOCATION" on page 1119.

Confirmation Command

"SHOW LOCATION" on page 1138

Examples

This example creates a new civic location entry that has the following specifications:

ID number: 5
Address: 100 New Adams Way
             Floor 2, wiring closet 214
             San Jose, CA 95134

```
awplus> enable
awplus# configure terminal
awplus(config)# location civic-location identifier 5
awplus(config_civic)# country US
awplus(config_civic)# city San-Jose
awplus(config_civic)# state CA
awplus(config_civic)# building 100
awplus(config_civic)# primary-road-name New-Adams
awplus(config_civic)# street-suffix Way
awplus(config_civic)# postal-code 95134
awplus(config_civic)# floor 2
awplus(config_civic)# room 214
awplus(config_civic)# exit
awplus(config)#
```

This example removes the defined values for the neighborhood and street-group parameters from LLDP-MED civic location ID 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# location civic-location identifier 3
awplus(config_civic)# no neighborhood
awplus(config_civic)# no street-group
awplus(config_civic)# exit
awplus(config)#
```

LOCATION COORD-LOCATION

Syntax

```
location coordinate-location identifier id_number
```

Parameters

id_number

Specifies an ID number for an LLDP-MED coordinate location entry. The range is 1 to 256. (This range is independent from the ID number ranges for civic and ELIN location entries.) You can specify only one ID number.

Mode

Global Configuration mode

Description

Use this command to create or modify LLDP-MED coordinate location entries on the switch. This command moves you to the Coordinate Location mode which contains the parameters you use to define the entries. The parameters are listed in Table 103.

Table 103. LLDP-MED Coordinate Location Entry Parameters

Parameter	Value
latitude	Latitude value in decimal degrees The range is -90.0º to 90.0º. The parameter accepts up to eight digits to the right of the decimal point.
lat-resolution	Latitude resolution as the number of valid bits. The range is 0 to 34 bits.
longitude	Longitude value in decimal degrees. The range is -180.0º to 180.0º. The parameter accepts up to eight digits to the right of the decimal point.
long-resolution	Longitude resolution as the number of valid bits. The range is 0 to 34 bits.

Table 103. LLDP-MED Coordinate Location Entry Parameters (Continued)

Parameter	Value
altitude floors	Altitude in number of floors. The range is -2097151.0 to 2097151.0. The value for this parameter must be specified between the two keywords, as shown here: altitude *n* floors
altitude meters	Altitude in meters. The range is -2097151.0 to 2097151.0 meters. The parameter accepts up to eight digits to the right of the decimal point. The value for this parameter must be specified between the two keywords, as shown here: altitude *n* meters
alt-resolution	Altitude resolution as the number of valid bits. The range is 0 to 30 bits.
datum nad83-mllw|nad83-navd|wgs84	The geodetic system (or datum) of the coordinates. The selections are: ❒ nad83-mllw - Mean lower low water datum 1983 ❒ nad83-navd - North American vertical datum 1983 ❒ wgs84 - World Geodetic System 1984

This command is also used to remove parameter values from existing LLDP-MED coordinate location entries. To remove parameters, use the NO forms of the parameters listed in Table 103.

To assign coordinate location entries to ports, refer to "LLDP LOCATION" on page 1087.

To remove a coordinate location entry, use "NO LOCATION" on page 1119.

Confirmation Command

"SHOW LOCATION" on page 1138

Examples

This example creates a new coordinate location entry with these specifications.

ID number: 16
Latitude: 37.29153547
Longitude: --121.91528320
Datum: nad83-navd
Altitude: 10.25 meters

```
awplus> enable
awplus# configure terminal
awplus(config)# location coord-location identifier 16
awplus(config_coord)# latitude 37.29153547
awplus(config_coord)# longitude -121.91528320
awplus(config_coord)# datum nad83-navd
awplus(config_coord)# altitude 10.25 meters
awplus(config_coord)# exit
```

This example removes the datum and altitude values without assigning new values from LLDP-MED civic location ID 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# location coord-location identifier 3
awplus(config_coord)# no datum
awplus(config_coord)# no altitude
awplus(config_coord)# exit
```

LOCATION ELIN-LOCATION

Syntax

```
location elin-location elin_id identifier id_number
```

Parameters

elin_id
> Specifies the ELIN (Emergency Location Identification Number) of 10 to 25 digits.

id_number
> Specifies an ID number for an LLDP-MED coordinate location entry on the switch. The range is 1 to 256. (This range is separate from the ranges for civic and coordinate entries.) You can specify only one ID number.

Mode

Global Configuration mode

Description

Use this command to create or modify LLDP-MED ELIN location entries on the switch. To create a new ELIN TLV, specify an unused ID number. To modify an existing ELIN TLV, enter its ID number.

To assign ELIN location entries to ports on the switch, use "LLDP LOCATION" on page 1087.

To remove an ELIN location entry, use "NO LOCATION" on page 1119.

Confirmation Command

"SHOW LOCATION" on page 1138

Example

This example creates a new location entry for ELIN 1234567890, with the ID number 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# location elin-location 1234567890 identifier
15
```

NO LLDP MED-NOTIFICATIONS

Syntax

```
no lldp med-notifications
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to configure the switch not to send LLDP-MED topology change notifications when devices are connected to or disconnected from the specified ports.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Example

This example configures the switch not to send LLDP-MED topology change notifications when devices are connected to or removed from port 19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.19
awplus(config-if)# no lldp med-notifications
```

NO LLDP MED-TLV-SELECT

Syntax

```
no lldp med-tlv-select capabilities/network-
policy/location/power-management-ext/inventory-
management/all
```

Parameters

capabilities
> Specifies the capabilities TLV.

network-policy
> Specifies the network policy TLV.

location
> Specifies the location identification TLV.

power-management-ext
> Specifies the extended power-via-MDI TLV.

inventory-management
> Specifies the inventory management TLV.

all
> Configures a port to stop sending all LLDP-MED TLVs.

Mode

Port Interface mode

Description

Use this command to stop ports from transmitting LLDP-MED TLVs. You can specify only one TLV per command. The default setting is for ports to send all optional LLDP-MED TLVs, except for the inventory TLV.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Examples

This example stops port 8 from transmitting all LLDP-MED TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# no lldp med-tlv-select all
```

This example stops ports 2 and 16 from transmitting the LLDP-MED capabilities and network policy TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2,port1.0.16
awplus(config-if)# no lldp med-tlv-select capabilities
awplus(config-if)# no lldp med-tlv-select network-policy
```

NO LLDP NOTIFICATIONS

Syntax

```
no lldp notifications
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to prevent ports from sending LLDP SNMP notifications (traps).

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Example

This example prevents port 14 from transmitting SNMP notifications:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# no lldp notifications
```

NO LLDP RUN

Syntax

```
no lldp run
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable LLDP and LLDP-MED on the switch. The switch, when LLDP and LLDP-MED are disabled, neither sends advertisements to nor collects information from its neighbors. The LLDP settings are retained by the switch.

Confirmation Command

"SHOW LLDP" on page 1121

Example

This example disables LLDP and LLDP-MED on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no lldp run
```

NO LLDP TLV-SELECT

Syntax

no lldp tlv-select *all/tlv*

Parameters

all

> Removes all optional LLDP TLVs from a port.

tlv

> Removes an optional TLV from a port. You can specify only one TLV. To remove more than one TLV from a port, repeat the command as many times as needed.

Mode

Port Interface mode

Description

Use this command to stop ports from sending optional LLDP TLVs to their neighbors. The optional TLVs are listed in Table 101 on page 1100.

To stop ports from transmitting LLDP-MED TLVs, refer to "NO LLDP MED-TLV-SELECT" on page 1113.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Examples

This example configures ports 21 and 22 to stop transmitting all optional LLDP TLVs:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.21,port1.0.22
awplus(config-if)# no lldp tlv-select all
```

This example stops the transmission of the management-address and system-capabilities TLVs on port 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11
awplus(config-if)# no lldp tlv-select management-address
awplus(config-if)# no lldp tlv-select system-capabilities
```

1117

NO LLDP TRANSMIT RECEIVE

Syntax

```
no lldp transmit/receive
```

Parameters

transmit

Stops ports from sending LLDP and LLDP-MED advertisements.

receive

Stops ports from accepting LLDP and LLDP-MED advertisements.

Mode

Port Interface mode

Description

Use this command to stop ports from transmitting and/or accepting LLDP and LLDP-MED advertisements to or from their neighbors.

Confirmation Command

"SHOW LLDP INTERFACE" on page 1123

Examples

This example stops port 12 from transmitting or receiving LLDP advertisements:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no lldp transmit receive
```

This example configures ports 3 and 4 to stop receiving LLDP advertisements:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3-port1.0.4
awplus(config-if)# no lldp receive
```

NO LOCATION

Syntax

```
no location civic-location|coord-location|elin-location
identifier id_number
```

Parameters

civic-location

   Deletes a civic location from the switch.

coord-location

   Deletes a coordinate location.

elin-location

   Deletes an ELIN location.

id_number

   Specifies the ID number of the location information to be deleted
   from the switch. You can specify only one location entry at a time.

Mode

Global Configuration mode

Description

Use this command to delete LLDP-MED location entries from the switch.
The same command is used to remove civic locations, coordinate
locations and ELIN locations. You can delete only one entry at a time.

Confirmation Command

"SHOW LOCATION" on page 1138

Examples

This example deletes the civic location ID 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# no location civic-location-id 17
```

This example removes the coordinate location IDs 6 and 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# no location coord-location-id 6
awplus(config)# no location coord-location-id 8
```

This example removes the ELIN location IDs 3 and 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# no location elin-location-id 3
awplus(config)# no location elin-location-id 4
```

SHOW LLDP

Syntax

show lldp

Parameters

None.

Mode

Privileged Exec mode

Description

Use this command to display general LLDP settings. Here is an example of the information.

```
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]
Fast Start Count .......... 3           [3]

LLDP Global Status:
Total Neighbor Count ...... 47
Neighbors table last updated 1 hrs 7 mins 6 secs ago
```

Figure 179. SHOW LLDP Command

The fields are defined in Table 104.

Table 104. SHOW LLDP Command

Field	Description
LLDP Status	Whether LLDP is enabled or disabled on the switch.
Notification Interval	Minimum interval between LLDP notifications.
Tx Timer Interval	Transmit interval between regular transmissions of LLDP advertisements.

1121

Table 104. SHOW LLDP Command (Continued)

Field	Description
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 re-initialization delay. This is the minimum time that must elapse after LLDP has been disabled before it can be initialized again.
Tx Delay	The transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information.
Total Neighbor Count	Number of LLDP neighbors the switch has discovered on all its ports.
Neighbors table last updated	The time since the LLDP neighbor table was last updated.

Example

The following example displays general LLDP settings:

```
awplus# show lldp
```

SHOW LLDP INTERFACE

Syntax

```
show lldp interface [port]
```

Parameters

port

Specifies a port, You can specify more than one port at a time with this command. Omitting this variable displays the LLDP settings for all ports.

Mode

Privileged Exec mode

Description

Use this command to display the LLDP port settings. Here is an example of the information.

```
LLDP Port Status and Configuration:
  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    Rx Tx  -- --  0.0.0.0         PdSmSdSc-- Pv--VnPi MpPoLaMf McNpLo--In
2    Rx Tx  -- --  0.0.0.0         PdSmSdSc-- Pv--VnPi MpPoLaMf McNpLo--In
3    Rx --  -- --  0.0.0.0         ---------- -------- -------- ----------
4    Rx Tx  -- --  149.124.36.15   PdSmSdScMa Pv--VnPi MpPoLaMf McNpLo--In
5    Rx Tx  -- --  149.124.36.15   PdSmSdScMa Pv--VnPi MpPoLaMf McNpLo--In
```

Figure 180. SHOW LLDP INTERFACE Command

Examples

This example displays the LLDP settings for all the ports on the switch:

```
awplus# show lldp interface
```

This example displays the LLDP settings for ports 5, 6 and 11:

```
awplus# show lldp interface port1.0.5,port1.0.6,port1.0.11
```

SHOW LLDP LOCAL-INFO INTERFACE

Syntax

show lldp local-info [interface *port*]

Parameters

port

Specifies a port, You can specify more than one port at a time with this command. Omitting this parameter displays the LLDP information for all the ports.

Mode

Privileged Exec mode

Description

Use this command to display the LLDP and LLDP-MED TLVs that the local ports are actively transmitting to their LLDP-compatible neighbors. Ports that have not been activated with "LLDP TRANSMIT RECEIVE" on page 1103 or that have not established links with their LLDP counterparts cannot be displayed with this command. See Figure 181 and Figure 182 on page 1126.

```
LLDP Local Information:
   Chassis ID Type .................. MAC address
   Chassis ID ....................... 0015.77d8.4360
   Port ID Type ..................... Port component
   Port ID .......................... 25
   TTL .............................. 120 (secs)
   Port Description ................. Port_25
   System Name ...................... [zero length]
   System Description ............... AT-9000/28
   System Capabilities   - Supported .. Bridge, Router
                         - Enabled .... Bridge, Router
   Management Addresses ............. 0.0.0.0
   Port VLAN ID (PVID) .............. 1
   Port & Protocol VLAN  - Supported . No
                         - Enabled ... No
                         - VIDs ...... 0
   VLAN Names ....................... Default_VLAN
   Protocol IDs .....................
   MAC/PHY Auto-negotiation .......... Supported / Enabled
        Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                      10BaseTFD, 10BaseT
        Operational MAU Type ........ 30 (1000BaseTFD)
```

Figure 181. SHOW LLDP LOCAL-INFO INTERFACE Command

```
    Power Via MDI (PoE) .............. Not Supported
    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, Inventory

    Network Policy ................... 1
         Application Type ........... Voice
         Frame Format ............... Untagged
         VLAN ID .................... 1
         Layer 2 Priority ........... 0
         DSCP Value ................. 0
    Location Identifier .............. [not advertised]
    Extended Power Via MDI (PoE) ..... Not Supported
    Inventory Information:
         Hardware Revision .......... A
         Firmware Revision .......... v1.0.0
         Software Revision .......... v1.0.0
         Serial Number .............. A04161H09020007
         Manufacturer Name .......... ATI
         Model Name ................. AT-9000/28SP
         Asset ID ................... [not advertised]
```

Figure 182. SHOW LLDP LOCAL-INFO INTERFACE Command
(continued)

The fields are defined in Table 105 on page 1128.

Examples

This example displays all ports that are actively transmitting TLVs:

awplus# show lldp local-info interface

This example displays the TLVs being actively transmitted by ports 18 and 23:

awplus# show lldp local-info interface port1.0.18,port1.0.23

SHOW LLDP NEIGHBORS DETAIL

Syntax

show lldp neighbors detail [interface *port*]

Parameters

port
> Specifies a port. You can specify more than one port.

Mode

Privileged Exec mode

Description

Use this command to display the information the switch has gathered from its LLDP and LLDP-MED neighbors. To display the information for all the neighbors, do not include the INTERFACE parameter. See Figure 183 and Figure 184 on page 1128.

```
LLDP Detailed Neighbor Information:
   Neighbors table last updated 0 hrs 0 mins 20 secs ago
   Chassis ID Type .................. MAC address
   Chassis ID ....................... 0015.77d8.4360
   Port ID Type ..................... Port component
   Port ID .......................... port1.0.25
   TTL .............................. 120 (secs)
   Port Description ................. Port 25
   System Name ...................... [zero length]
   System Description ............... AT-9000/28SP
   System Capabilities   - Supported .. Bridge, Router
                         - Enabled .... Bridge, Router
   Management Addresses ............. 0.0.0.0
   Port VLAN ID (PVID) .............. 1
   Port & Protocol VLAN  - Supported . No
                         - Enabled ... No
                         - VIDs ...... 0
   VLAN Names ....................... Default_VLAN
   Protocol IDs .....................
   MAC/PHY Auto-negotiation ......... Supported / Enabled
        Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                      10BaseTFD, 10BaseT
        Operational MAU Type ........ 30 (1000BaseTFD)
   Power Via MDI (PoE) .............. Not Supported
   Link Aggregation ................. Supported / Disabled
   Maximum Frame Size ............... 1522 (Octets)
```

Figure 183. SHOW LLDP NEIGHBORS DETAIL Command

```
    LLDP-MED Device Type ............. Network Connectivity
    LLDP-MED Capabilities ............ LLDP-MED Capabilities,
                                        Network Policy,
                                        Location Identification, Inventory
Network Policy ................... 1
        Application Type ........... Voice
        Frame Format ............... Untagged
        VLAN ID .................... 1
        Layer 2 Priority ........... 0
        DSCP Value ................. 0
Location Identifier .............. [not advertised]
Extended Power Via MDI (PoE) ..... Not Supported
Inventory Information:
        Hardware Revision .......... A
        Firmware Revision .......... v1.0.0
        Software Revision .......... v1.0.0
        Serial Number .............. A04161H09020007
        Manufacturer Name .......... ATI
        Model Name ................. AT-9000/52
        Asset ID ................... [not advertised]
```

Figure 184. SHOW LLDP NEIGHBORS DETAIL Command (continued)

The information is explained in Table 105.

Table 105. 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.
System Name	Neighbor's system name.
System Description	A description of the switch, such as the product name.
System Capabilities (Supported)	The device's functions supported by the switch.

Table 105. SHOW LLDP NEIGHBORS DETAIL Command (Continued)

Parameter	Description
System Capabilities (Enabled)	The device's functions, and whether or not these functions are currently enabled.
Management Address	The IP address of the neighbor.
Port VLAN ID (PVID)	The VLAN ID of the port.
Port & Protocol VLAN (Supported)	The protocol VLANs supported by the switch.
Port & Protocol VLAN (Enabled)	The protocol VLANs enabled on the switch.
Port & Protocol VLAN (VIDs)	The VLAN IDs of the protocol VLANs supported on the switch.
VLAN Names	The names of the port-based and tagged VLANs in which the neighbor port is a member.
Protocol IDs	List of protocols that are accessible through the neighbor's port.
MAC/PHY Auto-negotiation	The speed and duplex mode of the port and whether the port was configured with Auto-Negotiation.
Advertised Capability	The auto-negotiation port capabilities, including 1000BaseTDF, 100BaseTXFD, 100BaseTX, 10BaseTFD, 10BaseT.
Operational MAU Type	The Operational MAU (Medium Attachment Unit) type is the attached device's medium speed such as twisted pair, fiber, or link speed.
Power via MDI (PoE)	The power via MDI capabilities of the port.
Link Aggregation	The link aggregation status.
Maximum Frame Size	The maximum frame size the port can forward.
LLDP-MED Device Type	The LLDP-MED device types are Class I, Class II, Class III, Network Connectivity, Local, and Unknown.
LLDP-MED Capabilities	The LLDP-MED TLVs that are supported and enabled on the switch, and the device type, which for this switch is Network Connectivity Device.

Table 105. SHOW LLDP NEIGHBORS DETAIL Command (Continued)

Parameter	Description
Network Policy	The 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 Class of Service (CoS) priority Voice VLAN Diffserv Code Point (DSCP)
Application Type	The switch supports Application Type 1: Voice.
Frame Format	The frame format specifies the port type connected to a VLAN as tagged or untagged.
VLAN ID	The Virtual Local Area Network ID (VID).
Layer 2 Priority	Layer 2 user priority is in the range of 0 to 7.
DSCP Value	Indicates a DSCP priority level. The range is 0 to 63. A level of 0 is the lowest priority, and a level of 63 is the highest priority.
Location Identifier	Specifies an ID number for an LLDP-MED civic location entry on the switch. The range is 1 to 256.
Extended Power via MDI (PoE)	The extended power via MDI capabilities of the port.
Inventory Information	
Hardware Revision	The hardware revision number of the chassis.
Firmware Revision	The revision number of the bootloader on the chassis.
Software Revision	The revision number of the management software on the chassis.
Serial Number	The serial number of the device.

Table 105. SHOW LLDP NEIGHBORS DETAIL Command (Continued)

Parameter	Description
Manufacturer Name	The name of the company that manufactured the device.
Model Name	The model name.
Asset ID	The asset ID number.

Examples

This example displays the information from all of the neighbors on the switch:

```
awplus# show lldp neighbors
```

This example displays the information from all of the neighbors that are connected to ports 1 and 4:

```
awplus# show lldp neighbors interface port1.0.1,port1.0.4
```

SHOW LLDP NEIGHBORS INTERFACE

Syntax

```
show lldp neighbors interface [port]
```

Parameters

port

Specifies a port. You can specify more than one port at a time with this command.

Mode

Privileged Exec mode

Description

Use this command to view a summary of the information gathered by the switch from its LLDP and LLDP-MED neighbors. To display the information from all the neighbors, do not include a port number.

```
Total number of neighbors on these ports .... 1

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 Class 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 Name  Sys Name                    Cap.        Cl Pwr
-----------------------------------------------------------------------------
1.0.2   0015.77cc.e242     1.0.12                                 --B-R---
1.0.3   c286.11bc.a7a4     1.0.16                                 --B-R---
```

Figure 185. SHOW LLDP NEIGHBORS INTERFACE Command

The information is explained in Table 106.

Table 106. SHOW LLDP NEIGHBORS INTERFACE Command

Parameter	Description
Local Port	The local port that received the information from the neighbor.
Neighbor Chassis ID	The ID number of the neighbor's chassis.

Table 106. SHOW LLDP NEIGHBORS INTERFACE Command

Parameter	Description
Neighbor Port Name	The number of the neighbor's port that sent the information.
Neighbor System Name	The neighbor's system name.
Neighbor Capability	Capabilities that are supported and enabled on the neighbor.

Examples

This example displays a summary of the information from all the neighbors connected to the switch:

```
awplus# show lldp neighbors interface
```

This example displays a summary of the information from the neighbors connected to ports 1 and 4:

```
awplus# show lldp neighbors interface port1.0.1,port1.0.4
```

SHOW LLDP STATISTICS

Syntax

show lldp statistics

Parameters

None

Mode

User Exec mode and Privileged Exec mode

Description

Use this command to display the LLDP statistics for the switch. Here is an example of the information.

```
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
```

Figure 186. SHOW LLDP STATISTICS Command

The information the command displays is explained in Table 107.

Table 107. SHOW LLDP STATISTICS Command

Statistic	Description
Frame Out	Number of LLDPDU frames transmitted.
Frame In	Number of LLDPDU frames received.
Frame In Errored	Number of invalid LLDPDU frames received.
Frame In Dropped	Number of LLDPDU frames received and discarded.

1134

Table 107. SHOW LLDP STATISTICS Command (Continued)

Statistic	Description
TLVs Unrecognized	Number of LLDP TLVs received that were not recognized, but the TLV types were in the range of reserved TLV types
TLVs Discarded	Number of discarded TLVs.
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.

Example

The following example displays LLDP statistics for the switch:

```
awplus# show lldp statistics
```

SHOW LLDP STATISTICS INTERFACE

Syntax

```
show lldp statistics interface [port]
```

Parameters

port
> Specifies a port. You can specify more than one port.

Mode

User Exec mode and Privileged Exec mode

Description

Use this command to display the LLDP statistics for the individual ports. Here is an example of the information.

```
LLDP Packet and Event counters:

Port 2.0.2
   Frames:     Out ................... 15
               In .................... 12
               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
```

Figure 187. SHOW LLDP STATISTICS INTERFACE Command

The information the command displays is explained in Table 108.

Table 108. SHOW LLDP STATISTICS INTERFACE Command

Statistic	Description
Frame Out	Number of LLDPDU frames transmitted by the port.
Frame In	Number of LLDPDU frames received by the port.
Frame In Errored	Number of invalid LLDPDU frames received by the port.

1136

Table 108. SHOW LLDP STATISTICS INTERFACE Command

Statistic	Description
Frame In Dropped	Number of LLDPDU frames the port received and discarded.
TLVs Unrecognized	Number of LLDP TLVs received that were not recognized, but the TLV types were in the range of reserved TLV types
TLVs Discarded	Number of TLVs discarded by the port.
Neighbors New Entries	Number of times the information advertised by the neighbor on the port has been inserted into the neighbor table.
Neighbors Deleted Entries	Number of times the information advertised by the neighbor on the port has been removed from the neighbor table.
Neighbors Dropped Entries	Number of times the information advertised by the neighbor on the port could not be entered into the neighbor table because of insufficient resources.
Neighbors Entry Age-outs Entries	Number of times the information advertised by the neighbor on the port has been removed from the neighbor table because the information TTL interval has expired.

Examples

This example displays the statistics for all the ports:

```
awplus# show lldp statistics interface
```

This example displays the statistics for ports 2, 6 and 18:

```
awplus# show lldp statistics interface
port1.0.2,port1.0.6,port1.0.18
```

SHOW LOCATION

Syntax

```
show location civic-location|coord-location|elin-location
[identifier id-number|interface port]
```

Parameters

id-number

  Specifies an ID number of a location entry.

port

  Specifies a port. You can specify more than one port.

Mode

User Exec mode and Privileged Exec mode

Description

Use this command to display the civic, coordinate or ELIN location entries on the switch. Here is an example of a civic location entry.

```
ID      Element Type          Element Value
------------------------------------------------
8       Country               US
        State                 CA
        City                  San-Jose
        Street Suffix         Avenue
        Postal Code           95132
        Building              1020
        Primary Road Name     Pineapple
```

Figure 188. SHOW LOCATION Command for a Civic Location

The information the command displays is explained in Table 109.

Table 109. SHOW LLDP STATISTICS INTERFACE Command

Column	Description
ID	The ID number of the entry.
Element Type	A parameter of the entry.
Element Value	The current value of a parameter.

1138

Examples

The following example displays all the civic location entries on the switch:

```
awplus# show location civic-location
```

The following example displays only civic location entry 8:

```
awplus# show location civic-location identifier 8
```

The following example displays the civic location entry assigned to port 13:

```
awplus# show location civic-location interface port1.0.13
```

The following example displays all the coordinate location entries:

```
awplus# show location coord-location
```

The following example displays only coordinate location entry 16:

```
awplus# show location coord-location identifier 16
```

The following example displays the coordinate location assigned to port 21:

```
awplus# show location coord-location interface port1.0.21
```

The following example displays all the ELIN location entries:

```
awplus# show location elin-location
```

The following example displays only ELIN location entry 3:

```
awplus# show location elin-location identifier 3
```

The following example displays the ELIN location entry assigned to port 23:

```
awplus# show location elin-location interface port1.0.23
```

Chapter 69

Address Resolution Protocol (ARP)

This chapter contains the following topics:

Overview

The Address Resolution Protocol (ARP) is used to associate an IPv4 address with a MAC address used by network nodes. ARP gathers information about mapping between an IPv4 address and a MAC address and stores them in the ARP cache. The ARP cache is located in the RAM of a node. When the node receives a packet from the Network layer, then the node encapsulates the packet into a frame. The node looks up the ARP cache to find out the MAC address of the destination node.

ARP on the Switch

The software supports the following settings:

❒ Dynamic ARP entries timeout in 300 seconds

❒ Up to 1024 static ARP entries

Dynamic ARP Entries

ARP entries that are gathered dynamically populate the ARP table in the cache. These are called dynamic ARP entries. Dynamic ARP entries are updated in two ways:

❒ During regular operations

When a node receives frames from the media, it records the source IP and MAC addresses.

❒ Using ARP broadcast requests

When a node creates a frame and does not find an entry of the destination IPv4 address in the ARP cache, ARP broadcasts a request, including the IP address of the destination host, to all the devices on the LAN. Only the node assigned to the IP address replies to the sender. Based on the reply, the original node makes an ARP entry into the ARP table in the ARP cache.

On the AT-9000 switches, the dynamic ARP entries are time-stamped and set to time out in 300 seconds.

Static ARP Entries

A manually entered ARP entry is called a static ARP entry. Static ARP entries never expire. You must remove them manually as needed.

The software can support up to 1024 static ARP entries.

Adding Static ARP Entries

In most cases, the ARP table can be populated dynamically; however, the switch allows you to add an ARP entry to the ARP cache manually because there are cases in which you want to add static ARP entries.

One case is when a node connected to the switch does not support ARP. The node does not reply to the ARP request that the switch broadcasts, and an ARP entry for the node cannot be created dynamically. Another case is when routes are fixed and not subject to change. Dynamic ARP entries time out, and ARP re-broadcasts ARP requests even when no change occurs in the network topology. By creating fixed routes statically, you can reduce ARP broadcasting requests.

To add a static ARP entry, use the ARP command in the Global Configuration mode. Here is the format of the command:

```
arp ipaddress macaddress port_number
```

You must include both the IP address and the MAC address of the destination node. The MAC address must be entered in one of the following formats:

❐ xx:xx:xx:xx:xx:xx

❐ zzzz.zzzz.zzzz

Note
The switch must have a management IP address to support static ARP entries. The IP addresses of the ARP entries must be members of the same subnet as the management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

The following example creates an ARP entry for the IP address 192.168.0.16 and the MAC address 2b:56:c2:78:62:a3 on port 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# arp 192.168.0.16 00:02:c2:78:62:a3
port1.0.16
```

Deleting Static and Dynamic ARP Entries

The ARP cache contains two types of ARP entries: dynamic and static. These types of ARP entries are deleted using different commands shown in Table 110.

Table 110. Deleting ARP Entries

To Do This Task	Use This Command
Delete dynamic ARP entries.	CLEAR ARP-CACHE
Delete static ARP entries.	NO ARP (IP ADDRESS)

The CLEAR ARP-CACHE command deletes all dynamic ARP entries at once.

The following example deletes all of the dynamic ARP entries in the ARP cache:

```
awplus> enable
awplus# clear arp-cache
```

You can delete one static ARP entry with the NO ARP (IP ADDRESS) command. The following example deletes the static ARP entry for the IP address 192.168.1.12:

```
awplus> enable
awplus# configure terminal
awplus(config)# no arp 192.168.1.12
```

1144

Displaying the ARP Table

To display the ARP table on the switch, use the SHOW ARP command in the User Exec mode or the Privileged Exec mode. Here is the format of the command:

```
awplus# show arp
```

An example is shown in Figure 189.

```
IP ARP

ARP Cache Timeout ......... 300 seconds

Total ARP Entries ......... 215

IP Address      MAC Address      Interface   Port        Type
-----------------------------------------------------------------
149.122.34.4    0006.5bb2.4421   vlan2       port1.0.2   Dynamic
149.122.34.12   00a0.d218.eea1   vlan2       port1.0.3   Dynamic
149.122.34.21   00a0.c357.3214   vlan2       port1.0.4   Dynamic
149.122.35.1    00a0.64b1.76a5   vlan8       port1.0.7   Dynamic
```

Figure 189. SHOW ARP Command

The fields are described in Table 112 on page 1152.

1146

Chapter 70

Address Resolution Protocol (ARP) Commands

The ARP commands are summarized in Table 111 and described in detail within the chapter.

Table 111. ARP Commands

Command	Mode	Description
"ARP" on page 1148	Global Configuration	Adds static ARP entries to the ARP cache.
"CLEAR ARP-CACHE" on page 1150	User Exec and Privileged Exec	Deletes all dynamic ARP entries from the ARP cache.
"NO ARP (IP ADDRESS)" on page 1151	Global Configuration	Deletes a static ARP entry from the ARP cache.
"SHOW ARP" on page 1152	User Exec and Privileged Exec	Displays the static and dynamic ARP entries in the ARP cache.

1147

ARP

Syntax

arp *ipaddress macaddress port_number*

Parameters

ipaddress
    Specifies the IP address of the host.

macaddress
    Specifies the MAC address of the host. The MAC address must be entered in one of the following formats:

    xx:xx:xx:xx:xx:xx
    or
    zzzz.zzzz.zzzz

port_number
    Specifies the port number associated with the IP address.

Mode

Global Configuration mode

Description

Use this command to add the static ARP entry of a host to the ARP cache. The ARP entry must not already exist in the ARP cache. The switch can support up to 1024 static ARP entries.

Note
The switch must have a management IP address to support static ARP entries. The IP addresses of the ARP entries must be members of the same subnet as the management IP address. To assign an management IP address to the switch, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

Confirmation Command

"SHOW ARP" on page 1152

Example

The following example creates an ARP entry for the IP address 192.168.1.3 and the MAC address 7a:54:2b:11:65:72 on port 25:

```
awplus> enable
awplus# configure terminal
awplus(config)# arp 192.168.1.3 7a:54:2b:11:65:72 port1.0.25
```

CLEAR ARP-CACHE

Syntax

```
clear arp-cache
```

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to delete all dynamic ARP entries from the ARP cache on the switch.

Confirmation Command

"SHOW ARP" on page 1152

Example

The following example deletes all of the ARP entries dynamically added to the ARP cache:

```
awplus> enable
awplus# clear arp-cache
```

NO ARP (IP ADDRESS)

Syntax

`no arp `*`ipaddress`*

Parameters

ipaddress
>   Specifies the IP address of a static ARP entry.

Mode

Global Configuration mode

Description

Use this command to delete a static ARP entry from the ARP cache. Static ARP entries do not expire, and you must remove them manually. This command can delete only one ARP entry at a time.

Confirmation Command

"SHOW ARP" on page 1152

Example

The following example deletes the static ARP entry of the IP address 192.168.1.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no arp 192.168.1.2
```

SHOW ARP

Syntax

```
show arp
```

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display the ARP entries in the ARP cache.
Figure 190 is an example of the information displayed by this command.

```
IP ARP

ARP Cache Timeout ......... 300 seconds

Total ARP Entries ......... 2

IP Address     MAC Address            Interface    Port        Type
------------------------------------------------------------------
10.0.0.1       eccd.6d41.9e57         vlan1        port1.0.10  Dynamic
10.0.0.150     000c.2957.96db         vlan1        port1.0.10  Dynamic
10.0.0.75      0000.1a2a.f8bb         vlan1        port1.0.1   Static
```

Figure 190. SHOW ARP Command

The columns of the ARP table are described in Table 112.

Table 112. SHOW ARP Command

Parameter	Description
IP Address	Indicates the IP address of the host.
MAC Address	Indicates the MAC address of the host.
Interface	Indicates the VLAN where the host is a member.
Port	Indicates the port number where the host is connected.

1152

Table 112. SHOW ARP Command (Continued)

Parameter	Description
Type	Indicates the type of entry. The type is one of the following: ❒ Static: Static entry added with the ARP (IP ADDRESS MAC ADDRESS) command. ❒ Dynamic: Dynamic entry learned from ARP request/reply exchanges. ❒ Invalid: Possible nonexistent entry. ❒ Other: Entry automatically generated by the system.

Example

The following example displays the ARP entries in the ARP cache on the switch:

```
awplus# show arp
```

Chapter 71

RMON

This chapter contains the following topics:

Overview

The RMON (Remote MONitoring) MIB is used with SNMP applications to monitor the operations of network devices. The switch supports the four RMON MIB groups listed here:

❐ Statistic group. This group is used to view port statistics remotely with SNMP programs. For instructions, refer to "RMON Port Statistics" on page 1157.

❐ History group. This group is used to collect histories of port statistics to identify traffic trends or patterns. For instructions, refer to "RMON Histories" on page 1159.

❐ Alarm group. This group is used to create alarms that trigger event log messages or SNMP traps when statistics thresholds are exceeded. For instructions, refer to "RMON Alarms" on page 1162.

❐ Event group. This group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed. For instructions, refer to "RMON Alarms" on page 1162.

For instructions on how to configure SNMP on the switch, refer to Chapter 62, "SNMPv1 and SNMPv2c" on page 963 or Chapter 63, "SNMPv1 and SNMPv2c Commands" on page 975.

RMON Port Statistics

To view port statistics using an SNMP program and the RMON section in the MIB, you must configure the switch to reserve areas of memory in which to store the statistics for remote viewing with your SNMP program. These areas of memory are referred to as statistics groups. The switch can have up to eight statistics groups, and each group can store the statistics of a single port. Thus, you can remotely monitor up to eight ports at a time with an SNMP program. (To view the statistics of all the ports, use "SHOW PLATFORM TABLE PORT COUNTERS" on page 229.)

The following sections explain the commands for managing statistics groups:

❐ "Adding Statistics Groups" next

❐ "Viewing Statistics Groups" on page 1158

❐ "Deleting Statistics Groups" on page 1158

Adding Statistics Groups

The command to create statistics groups is the RMON COLLECTION STATS command in the Port Interface mode. Here is the format of the command:

```
rmon collection stats stats_id [owner owner]
```

The STATS_ID parameter is the ID number of the new group. The range is 1 to 65535. The groups will be easier to identify if their ID numbers are the same as the port numbers. For instance, a group assigned to port 16 should be assigned the ID number 16. You will find this particularly useful when you view the statistics with your SNMP program, because they are identified by the statistics group ID numbers and not by the port numbers. If the two numbers are different, you might have difficulty determining which port statistics you are viewing.

The OWNER parameter, used to identify the person who created an entry, is primarily intended for switches that are managed by more than one person, and is optional.

This example of the command assigns RMON statistics groups to ports 5, 16 and 20. The groups are assigned ID numbers that match the port numbers:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# rmon collection stats 5
awplus(config-if)# exit
awplus(config)# interface port1.0.16
```

```
awplus(config-if)# rmon collection stats 16
awplus(config-if)# exit
awplus(config)# interface port1.0.20
awplus(config-if)# rmon collection stats 20
```

You can now use your SNMP program and the RMON section of the MIB tree to view the RMON statistics of the ports. This assumes, of course, that SNMP is activated and configured on the switch.

Viewing Statistics Groups

To confirm the configuration, use the SHOW RMON STATISTICS command in the Privilege Exec mode:

```
awplus# show rmon statistics
```

Here is an example of the information.

```
Stats Index = 5
   Data source ifindex = 5
   Owner Agent

Stats Index = 16
   Data source ifindex = 16
   Owner Agent

Stats Index = 20
   Data source ifindex = 20
   Owner Agent
```

Figure 191. SHOW RMON STATISTICS Command

The fields are described in Table 119 on page 1194.

Deleting Statistics Groups

To delete RMON statistics groups from the ports on the switch, use the NO RMON COLLECTION STATS command in the Port Interface mode. This example of the command removes the group from port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no rmon collection stats 5
```

1158

RMON Histories

RMON histories are snapshots of port statistics. They are taken by the switch at predefined intervals and can be used to identify trends or patterns in the numbers or types of ingress packets on the ports on the switch. The snapshots can be viewed with your SNMP program, in the history group of the RMON portion of the MIB tree. (Port histories cannot be viewed through the command line interface.)

The switch stores the snapshots in areas of memory called history groups. There can be up to eight history groups on the switch and each group is capable of storing the snapshots of one port. Consequently, the switch can maintain the histories of up to eight ports at a time.

A history group is further divided into what are called buckets. Each bucket stores one snapshot of statistics of a port. A group can have from 1 to 50 buckets. The more buckets in a group, the more snapshots it can store.

The following sections explain how to manage RMON histories:

❑ "Adding History Groups" next
❑ "Displaying History Groups" on page 1160
❑ "Deleting History Groups" on page 1161

Adding History Groups

The command for creating history groups is the RMON COLLECTION HISTORY command. This command is in the Port Interface mode because history groups are applied on a per-port basis. Here is the format of the command:

```
rmon collection history history_id [buckets buckets]
[interval interval] [owner owner]
```

You can apply a history group to only one port.

The HISTORY_ID number is a history group's ID number. The range is 1 to 65535. As with statistics groups, which are explained earlier in this chapter, history groups are easier to identify when you view them with your SNMP program if their ID numbers are the same as the port numbers. This is because the SNMP program identifies the histories by the group numbers and not by the port numbers.

The BUCKETS variable defines the number of snapshots the switch is to store of the statistics of a port. Each bucket can store one snapshot of RMON statistics. Different ports can have different numbers of buckets. The range is 1 to 50 buckets.

The INTERVAL parameter, which is entered in seconds, specifies how frequently the switch is to take snapshots of the statistics. The range is 1 to 3600 seconds (1 hour). For example, if you want the switch to take one

1159

snapshot every minute for five minutes on a port, you specify five buckets (one bucket for each minute) and an interval of sixty seconds.

After you enter the command, the switch checks its memory to determine whether it has sufficient memory resources to create the history group. If its memory resources are insufficient, it reduces the number of buckets to an amount that can be accommodated by the resources. If there are no available resources, the switch cancels the history group.

The switch takes the first snapshot at the end of the first interval. A history group that has an interval of 1800 seconds, for example, does not take its first snapshot for 30 minutes. Once all the buckets of a group are full, the switch continues storing snapshots by deleting the oldest snapshots as it adds new snapshots. For instance, for a history group of three buckets, the switch deletes the first bucket when it adds the fourth bucket.

To stop a history from gathering any more statistics, you must delete it.

This example configures the switch to take a snapshot of the statistics of port 23 once every hour for fifteen hours:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# rmon collection history 23 buckets 15
interval 3600
```

This example of the command configures the switch to take a snapshot of the statistics of port 7 once every thirty minutes for four hours. Eight buckets are required because there are eight thirty minute periods in four hours:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# rmon collection history 7 buckets 8
interval 1800
```

Displaying History Groups

You should always check the configuration of a new history entry, just to be sure the switch had adequate memory resources. The command for displaying the entries is the SHOW RMON HISTORY command in the Privileged Exec mode:

```
awplus# show rmon history
```

Here is an example of the information.

```
History Index = 7
   Data source ifindex = 7
   Buckets requested = 8
   Buckets granted = 8
   Interval = 1800
   Owner Agent

History Index = 23
   Data source ifindex = 23
   Buckets requested = 15
   Buckets granted = 15
   Interval = 3600
   Owner Agent
```

Figure 192. SHOW RMON HISTORY Command

The fields are defined in Table 118 on page 1192.

Deleting History Groups

Use the NO RMON COLLECTION HISTORY command in the Port Interface mode to delete history groups from the switch. The switch stops collecting port statistic histories as soon as you enter the command. This example of the command deletes the history group with the ID 2 on port 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection history 2
```

RMON Alarms

RMON alarms are used to generate alert messages when packet activity on designated ports rises above or falls below specified threshold values. The alert messages can take the form of messages that are entered in the event log on the switch or traps that are sent to SNMP programs.

The switch supports up to eight alarms. Each RMON alarm can monitor one port and one RMON statistic.

RMON alarms consist of two thresholds. There is a rising threshold and a falling threshold. The alarm is triggered if the value of the monitored RMON statistic of the designated port exceeds the rising threshold. The response of the switch is to enter a message in the event log, send an SNMP trap, or both. The alarm is reset if the value of the monitored statistic drops below the falling threshold.

The frequency with which the switch tests the thresholds in an alarm against the actual RMON statistic is controlled by the time interval, a setting you can adjust for each alarm.

Here are the three components that comprise RMON alarms:

❐ RMON statistics group: A port must have an RMON statistics group if it is to have an alarm. When you create an alarm, you specify the port to which it is to be assigned not by the port number, but rather by the ID number of the port's statistics group. (As explained in "RMON Port Statistics" on page 1157, statistics groups are also used to remotely view port statistics in the RMON portion of the MIB tree.)

❐ RMON event: An event specifies the action of the switch when the ingress packet activity on a port crosses a statistic threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP workstation, or both. You can create up to eight events. Since there are only three possible actions, and since events can be used with more than one alarm, you probably will not create more than three events.

❐ Alarm: The last component is the alarm itself. It defines the port statistic to be monitored and the rising and falling thresholds that trigger the switch to perform an event. The thresholds of an alarm can have the same event or different events. The switch supports up to eight alarms.

The following sections explain how to create and manage the various elements of an alarm:

❒ "Creating RMON Statistics Groups" next

❒ "Creating RMON Events" on page 1163

❒ "Creating RMON Alarms" on page 1164

❒ "Creating an Alarm - Example 1" on page 1165

❒ "Creating an Alarm - Example 2" on page 1167

Creating RMON Statistics Groups

The port of an alarm must have an RMON statistics group. Statistics groups are created with the RMON COLLECTION STATS command, described in "RMON Port Statistics" on page 1157. Refer there for instructions on how to create the groups.

Creating RMON Events

The event of an alarm defines the action of the switch when a threshold is crossed. There are three commands for creating RMON events, one command for each action. Here is the command that creates events that enter messages in the event log when statistic thresholds are crossed:

rmon event *event_id* log description *description* [owner *owner*]

Here is the command to create events that send SNMP traps:

rmon event *event_id* trap *community_string* [description *description*] [owner *owner*]

This command creates events that both send SNMP traps and enter messages in the event log:

rmon event *event_id* log trap *community_string* [description *description*] [owner *owner*]

The EVENT_ID parameter is a value from 1 to 65535 that uniquely identifies the event.

The COMMUNITY_STRING parameter in the two commands that send SNMP traps identifies an SNMP community string on the switch. The designated community string should have host IP addresses of SNMP workstations that are to receive traps from the alarm. This parameter is case sensitive, and the community string must already exist on the switch. You can specify only one community string.

Using the DESCRIPTION parameter to describe the event makes the event easier to identify. The description can be up to 20 alphanumeric characters. Spaces and special characters are not allowed. This parameter is optional on the two commands that create events that send SNMP traps, but is required in the command that creates an event that only enters a log message.

The owner parameter is useful in situations where more than one person is managing the switch. You can use it to identify who created the event. This parameter is optional in all three commands.

Creating RMON Alarms

After you have added a statistics group to a port and created the event, you are ready to create the alarm with the RMON ALARM command, located in the Global Configuration mode. Here is the format of the command:

```
rmon alarm alarm_id oid.stats_id interval interval
delta|absolute rising-threshold rising-threshold event
rising_event_id falling-threshold falling-threshold event
falling_event_id [owner owner]
```

The ALARM_ID parameter is a value from 1 to 65535 that uniquely identifies the alarm. (Remember, the switch is limited to eight alarms at one time.)

The OID.STATS_ID parameter has two parts. The first part specifies the OID of the RMON statistic the alarm is to monitor. You have to specify the statistic by its OID. For example, the OID for etherStatsOctets is 1.3.6.1.2.1.16.1.1.1.4.

Table 113 is a partial list of the MIB object names and numbers for use in the OID portion of the variable. For the complete list, refer to Table 115 on page 1178.

Table 113. Abbreviated List of MIB Object Names and OID Numbers

MIB Name	OID Number
etherStatsDropEvents	1.3.6.1.2.1.16.1.1.1.3.*stats_id*
etherStatsOctets	1.3.6.1.2.1.16.1.1.1.4.*stats_id*
etherStatsPkts	1.3.6.1.2.1.16.1.1.1.5.*stats_id*
etherStatsBroadcastPkts.*stats_id*	1.3.6.1.2.1.16.1.1.1.6.*stats_id*
etherStatsMulticastPkts.*stats_id*	1.3.6.1.2.1.16.1.1.1.7.*stats_id*

The second part of the OID.STATS_ID variable is the ID number of the statistics group on the port the alarm is to monitor. The port is specified indirectly in the command, by the ID number of the statistics group. For example, if the alarm is to monitor port 4, use the STATS_ID variable to enter the ID number of the statistics group on port 4. If you follow the advice given earlier in this chapter, of always numbering statistics groups the same as the port numbers, the port numbers and the ID numbers of the statistics group should always be the same, thus lessening the chance of an alarm being assigned to the wrong port.

The INTERVAL parameter specifies how frequently the switch is to poll the statistics group to determine whether a threshold has been crossed.

The range is 1 to 65535 seconds.

The DELTA and ABSOLUTE parameters define the type of change that has to occur for the monitored statistic to trigger the alarm. The DELTA setting compares a threshold against the difference between the current and previous values of the statistic, while the ABSOLUTE setting compares a threshold against the current value of the statistic.

The raising and falling thresholds are the values which, when crossed, cause the switch to perform the specified events. The range for both thresholds is 1 to 65535.

The OWNER parameter is used to indicate who created the alarm. This parameter is optional.

Creating an Alarm - Example 1

This example creates an alarm that monitors the change per minute in the number of all ingress packets for port 22. The RMON statistic is etherStatsPkts, and its OID is 1.3.6.1.2.1.16.1.1.1.5. The alarm is assigned the ID number 1 and triggers event 3, which enters a message in the event log if the ingress traffic on the port exceeds 20000 packets per minute or falls below 1000 packets.

The first sequence of steps adds an RMON statistics group to port 22. The alarm will not work unless the switch is gathering statistics from the port to use with RMON. (You can skip this phase if the port already has a statistics group.)

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.22`	Enter the Port Interface mode for port 22.
`awplus(config-if)# rmon collection stats 22`	Add a statistics group to the port with the RMON COLLECTION STATS command. The entries are easier to remember if their ID numbers are the same as the port numbers to which they are assigned.
`awplus(config-if)# end`	Return to the Privileged Exec mode.
`awplus# show rmon statistics`	Use the SHOW RMON STATISTICS command to verify the configuration of the new group.

1165

The next series of steps creates the event, which enters a message in the event log whenever the thresholds are crossed:

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# rmon event 3 log description Enter_log_message`	Create the event with the RMON EVENT LOG command.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show rmon event`	Use the SHOW RMON EVENT command to verify the configuration of the new event.

Here are the specifications of the alarm:

❐ Alarm ID number 1

❐ Monitored statistic: etherStatsPkts - OID 1.3.6.1.2.1.16.1.1.1.5 (all ingress packets)

❐ Statistics group ID number: 22

❐ Interval: 60 seconds

❐ Rising threshold: 20000 packets

❐ Rising threshold event: 3

❐ Falling threshold: 1000 packets

❐ Falling threshold event: 3

Here are the steps to creating the alarm:

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.22 interval 60 delta rising-threshold 20000 event 3 falling-threshold 1000 event 3`	Create the alarm with the RMON ALARM command.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show rmon alarm`	Use the SHOW RMON ALARM command to verify the configuration of the new alarm.

Creating an Alarm - Example 2

This example creates an alarm that monitors the ingress broadcast traffic on port 20. The RMON statistic is etherStatsBroadcastPkts, and its OID is 1.3.6.1.2.1.16.1.1.1.6. The alarm triggers an event if the traffic exceeds 10,000 packets or falls below 1,000 packets per minute. Both thresholds have the same event, which logs a message in the event log and sends an SNMP trap when either threshold is crossed.

Phase 1: Creating the SNMP Community String and Activating SNMP

This example requires a community string because the event sends traps. The community string will be called "Station12ap" and will have the host ID addresses 149.211.243.12 and 149.211.243.75. Here are the steps to create the community string, assign it the IP addresses of the host nodes and activate SNMP on the switch.

`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# snmp-server`	Activate SNMP on the switch with the SNMP-SERVER command.
`awplus(config)# snmp-server enable trap`	Activate the transmission of traps with the SNMP-SERVER ENABLE TRAP command.
`awplus(config)# snmp-server community Station12ap rw`	Create the community string with the SNMP-SERVER COMMUNITY command.

awplus(config)# snmp-server host 149.211.243.12 traps version 2c Station12ap awplus(config)# snmp-server host 149.211.243.75 traps version 2c Station12ap	Add the IP addresses of the trap receivers to the community string with the SNMP-SERVER HOST command.
awplus(config)# exit	Return to the Privileged Exec mode.
awplus# show snmp-server	Verify that SNMP is enabled on the switch with the SHOW SNMP-SERVER command.
awplus# show snmp-server community	Verify the new community string with the SHOW SNMP-SERVER COMMUNITY command.
awplus# show running-config	Verify the host IP addresses of the community string with the SHOW RUNNING-CONFIG command.

Phase 2: Adding the RMON Statistics Group to the Port

The steps here add a statistics group to port 20 so that the port statistics are collected by the switch for use with RMON.

awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface port1.0.20	Enter the Port Interface mode for port 20.
awplus(config-if)# rmon collection stats 20	Add a statistics group to the port with the RMON COLLECTION STATS command. The groups are easier to remember when their ID numbers are the same as the port numbers.
awplus(config-if)# end	Return to the Privileged Exec mode.
awplus# show rmon statistics	Use the SHOW RMON STATISTICS command to verify the configuration of the new group.

Phase 3: Creating the Event

The event in this example is to send an SNMP trap and to log a message in the event log. The event is assigned the ID number 2.

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# rmon event 2 log trap Station12ap description trap_and_log_event`	Create the event with the RMON EVENT LOG TRAP command. It is important to remember that the community string is case sensitive.
`awplus(config)# exit`	Return to the Privileged Exec mode.
`awplus# show rmon event`	Use the SHOW RMON EVENT command to verify the configuration of the new event.

Phase 4: Creating the Alarm

Here are the specifications of the alarm:

- ❐ Alarm ID number 2
- ❐ Monitored statistic: etherStatsBroadcastPkts - OID 1.3.6.1.2.1.16.1.1.1.6 (broadcast packets)
- ❐ Statistics group ID number: 20
- ❐ Interval: 60 seconds
- ❐ Rising threshold: 10000 packets
- ❐ Rising threshold event: 2
- ❐ Falling threshold: 1000 packets
- ❐ Falling threshold event: 2

Here are the steps to creating the alarm.

`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# rmon alarm 2 1.3.6.1.2.1.16.1.1.1.6.20 interval 60 delta rising-threshold 10000 event 2 falling-threshold 1000 event 2`	Create the alarm with the RMON ALARM command.
`awplus(config)# exit`	Return to the Privileged Exec mode.

`awplus# show rmon alarm`	Use the SHOW RMON ALARM command to verify the new alarm.

Chapter 72

RMON Commands

The RMON commands are summarized in Table 114 and described in detail within the chapter.

Table 114. RMON Commands

Command	Mode	Description
"NO RMON ALARM" on page 1173	Global Configuration	Deletes alarms from the switch.
"NO RMON COLLECTION HISTORY" on page 1174	Port Interface	Deletes history groups from the ports on the switch.
"NO RMON COLLECTION STATS" on page 1175	Port Interface	Deletes statistics groups from the ports on the switch.
"NO RMON EVENT" on page 1176	Global Configuration	Deletes events from the switch.
"RMON ALARM" on page 1177	Global Configuration	Creates alarms to monitor RMON statistics on the ports.
"RMON COLLECTION HISTORY" on page 1180	Port Interface	Creates history groups on the ports.
"RMON COLLECTION STATS" on page 1182	Port Interface	Creates statistics groups on the ports.
"RMON EVENT LOG" on page 1183	Global Configuration	Creates alarm events that enter entries in the event log.
"RMON EVENT LOG TRAP" on page 1184	Global Configuration	Creates alarm events that enter entries in the event log and send SNMP traps.
"RMON EVENT TRAP" on page 1186	Global Configuration	Creates alarm events that send SNMP traps.
"SHOW RMON ALARM" on page 1188	Privileged Exec	Displays the RMON alarms on the switch.
"SHOW RMON EVENT" on page 1190	Privileged Exec	Displays the RMON events on the switch.

Table 114. RMON Commands (Continued)

Command	Mode	Description
"SHOW RMON HISTORY" on page 1192	Privileged Exec	Displays the RMON history groups that are assigned to the ports on the switch.
"SHOW RMON STATISTICS" on page 1194	Privileged Exec	Displays the statistics groups that are assigned to the ports.

NO RMON ALARM

Syntax

```
no rmon alarm alarm_id
```

Parameters

alarm_id
> Specifies the ID number of the alarm you want to delete. You can delete only one alarm at a time. The range is 1 to 65535.

Mode

Global Configuration mode

Description

Use this command to delete alarms from the switch.

Confirmation Command

"SHOW RMON ALARM" on page 1188

Example

This example deletes the alarm with ID 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# no rmon event 3
```

NO RMON COLLECTION HISTORY

Syntax

```
no rmon collection history collection_id
```

Parameters

collection_id
> Specifies the ID number of the history group you want to delete. You can delete only one group at a time. The range is 1 to 65535.

Mode

Port Interface mode

Description

Use this command to delete history groups from ports on the switch.

Confirmation Command

"SHOW RMON HISTORY" on page 1192

Example

This example deletes the history group that has the ID number 17 from port 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# no rmon collection history 17
```

NO RMON COLLECTION STATS

Syntax

```
no rmon collection stats stats_id
```

Parameters

stats_id
> Specifies the ID number of the statistics group you want to delete. The range is 1 to 65535.

Mode

Port Interface mode

Description

Use this command to delete statistics groups from ports on the switch.

Confirmation Command

"SHOW RMON STATISTICS" on page 1194

Example

This example deletes the statistics group with ID 11 from port 11:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11
awplus(config-if)# no rmon collection stats 11
```

NO RMON EVENT

Syntax

```
no rmon event event_id
```

Parameters

event_id
> Specifies the ID number of the event you want to delete from the switch. You can delete only one event at a time. The range is 1 to 65535.

Mode

Global Configuration mode

Description

Use this command to delete events from the switch.

Confirmation Command

"SHOW RMON EVENT" on page 1190

Example

This example delete the event with ID 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no rmon event 2
```

RMON ALARM

Syntax

rmon alarm *alarm_id oid.stats_id* interval *interval*
delta|absolute rising-threshold *rising-threshold* event
rising_event_id falling-threshold *falling-threshold* event
falling_event_id [owner *owner*]

Parameters

alarm_id

Specifies the ID number of a new alarm. The range is 1 to 65535.

oid

Specifies the OID of the RMON statistic the alarm should monitor.
You can specify just one statistic.

stats_id

Specifies the ID number of the statistics group that is assigned to
the port the alarm is to monitor. You can specify just one statistics
group, and the group must already exist.

For more information on the OID and STATS_ID variables, refer to
"Creating RMON Alarms" on page 1164.

interval

Specifies the polling interval in seconds. The range is 1 to 65535
seconds.

delta

Specifies that the alarm is based on the difference between the
current value and preceding value of the designated statistic.

absolute

Specifies that the alarm is based on the current value of the
designated RMON statistic.

rising_threshold

Specifies the rising threshold which, when crossed, causes the
switch to perform the specified event. The range is 1 to 65535.

rising_event_id

Specifies the ID number of the event the switch is to perform when
the rising threshold is crossed. The event must already exist.

falling_threshold

Specifies the falling threshold which, when crossed, causes the
switch to perform the specified event. The range is 1 to 65535.

rising_event_id
> Specifies the ID number of the event the switch is to perform when the falling threshold is crossed. The event must already exist.

owner
> Specifies the owner of the alarm.

Mode

Global Configuration mode

Description

Use this command to create RMON alarms. RMON alarms monitor the values of SNMP objects and trigger events when the values of the monitored objects cross specified thresholds. Here are the guidelines to this command:

❒ The switch supports up to eight alarms.

❒ An alarm can designate just one RMON statistic.

❒ An alarm can belong to just one port at a time.

❒ The port of an alarm must have an RMON statistics group. You must create the group before the alarm. For instructions, refer to "Adding Statistics Groups" on page 1157 or "RMON COLLECTION STATS" on page 1182.

❒ The port of an alarm is specified indirectly in the command. You use the STATS_ID parameter to specify the ID number of the RMON statistics group you added to the port.

❒ The command must include both rising and falling thresholds.

❒ The rising and falling thresholds can have different events or the same event. The events must already exist.

The OID parameter in the command specifies the OID of the MIB statistic the alarm is to monitor. The MIB object must be specified by its OID number. An alarm can have just one MIB object. Table 115 lists the possible object names and OID numbers. (The STATS_ID variable is the ID number of a statistics group through which the alarm monitors a port.)

Table 115. MIB Object Names and ID Numbers

MIB Name	OID Number
etherStatsDropEvents	1.3.6.1.2.1.16.1.1.1.3.*stats_id*
etherStatsOctets	1.3.6.1.2.1.16.1.1.1.4.*stats_id*
etherStatsPkts	1.3.6.1.2.1.16.1.1.1.5.*stats_id*
etherStatsBroadcastPkts	1.3.6.1.2.1.16.1.1.1.6.*stats_id*

Table 115. MIB Object Names and ID Numbers (Continued)

MIB Name	OID Number
etherStatsMulticastPkts	1.3.6.1.2.1.16.1.1.1.7.*stats_id*
etherStatsCRCAlignErrors	1.3.6.1.2.1.16.1.1.1.8.*stats_id*
etherStatsUndersizePkts	1.3.6.1.2.1.16.1.1.1.9.*stats_id*
etherStatsOversizePkts	1.3.6.1.2.1.16.1.1.1.10.*stats_id*
etherStatsFragments	1.3.6.1.2.1.16.1.1.1.11.*stats_id*
etherStatsJabbers	1.3.6.1.2.1.16.1.1.1.12.*stats_id*
etherStatsCollisions	1.3.6.1.2.1.16.1.1.1.13.*stats_id*
etherStatsPkts64Octets	1.3.6.1.2.1.16.1.1.1.14.*stats_id*
etherStatsPkts65to127Octets	1.3.6.1.2.1.16.1.1.1.15.*stats_id*
etherStatsPkts128to255Octets	1.3.6.1.2.1.16.1.1.1.16.*stats_id*
etherStatsPkts256to511Octets	1.3.6.1.2.1.16.1.1.1.17.*stats_id*
etherStatsPkts512to1023Octets	1.3.6.1.2.1.16.1.1.1.18.*stats_id*
etherStatsPkts1024to1518Octets	1.3.6.1.2.1.16.1.1.1.19.*stats_id*

Confirmation Command

"SHOW RMON ALARM" on page 1188

Example

This example creates an RMON alarm that monitors ingress multicast packets (OID 1.3.6.1.2.1.16.1.1.1.7) on a port assigned a statistics group with the ID number 5. The alarm triggers event ID number 1 if the number of multicast packets exceeds 10,000 packets per minute or falls below 1,000 packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.7.5
interval 60 delta rising-threshold 10000 event 1 falling-
threshold 1000 event 1
```

> **Note**
> For examples that illustrate how to create all of the components of RMON alarms, refer to "RMON Alarms" on page 1162.

RMON COLLECTION HISTORY

Syntax

```
rmon collection history history_id [buckets buckets]
[interval interval] [owner owner]
```

Parameters

history_id

Specifies the ID number of a new history group. The range is 1 to 65535.

buckets

Specifies the number of requested buckets to store snapshots. The range is 1 to 50 buckets.

interval

Specifies the polling interval in seconds. The range is 1 to 3600 seconds.

owner

Specifies an owner of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed.

Mode

Port Interface mode

Description

Use this command to add RMON history groups to the ports on the switch. History groups enable the switch to capture snapshots of the RMON statistics of the ports over time. You can view the snapshots with an SNMP program to look for trends or patterns in the numbers or types of ingress packets on the ports.

A history group can be applied to just one port, and the switch can support up to eight entries at a time. Thus, you can collect statistics histories on up to eight ports at a time.

The BUCKETS variable defines the number of snapshots the switch is to take of the RMON statistics of a port. Different ports can have different numbers of buckets. The INTERVAL parameter, which is entered in seconds, specifies how frequently the switch is to take the snapshots of the statistics. For example, if you want the switch to take one snapshot every minute for five minutes on a port, you would specify five buckets (one bucket for each minute) and an interval of sixty seconds.

1180

RMON statistics histories are only viewable from an SNMP application program. There are no commands in the command line interface for viewing histories.

Confirmation Command

"SHOW RMON HISTORY" on page 1192

Examples

This example creates a history group that takes a snapshot of the RMON statistics on port 14 every fifteen minutes (900 seconds) for two hours. The group requires eight buckets because there are eight fifteen-minute intervals in two hours. The group is assigned the ID number 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# rmon collection history 1 buckets 8
interval 900
```

This example creates a history group that takes a snapshot of the RMON statistics on port 7 every hour (3600 seconds) for twelve hours. The group, which is assigned the ID number 5, requires 12 buckets, one for each hour:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# rmon collection history 5 buckets 12
interval 3600
```

RMON COLLECTION STATS

Syntax

```
rmon collection stats stats_id [owner owner]
```

Parameters

stats_id
> Specifies the ID number of a new statistics group. The range is 1 to 65535.

owner
> Specifies an owner of up to 20 alphanumeric characters for the group. Spaces and special characters are not allowed.

Mode

Port Interface mode

Description

Use this command to create RMON statistics groups on the ports of the switch. The groups are used to view RMON port statistics from SNMP workstations on your network and to create RMON alarms.

A port can have only one RMON statistics group, and a group can be assigned to just one port at a time. The switch supports up to eight groups, allowing you to monitor up to eight ports at one time.

Confirmation Command

"SHOW RMON STATISTICS" on page 1194

Example

This example adds a statistics group to port 16 and assigns it the ID number 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# rmon collection stats 16
```

1182

RMON EVENT LOG

Syntax

```
rmon event event_id log description description [owner
owner]
```

Parameters

event_id
> Specifies the ID number of a new event. The range is 1 to 65535.

description
> Specifies a description of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed.

owner
> Specifies an owner of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed.

Mode

Global Configuration mode

Description

Use this command to create events for RMON alarms. This type of event enters a message in the event log when a rising or falling threshold of an alarm is crossed. The same event can be assigned to multiple alarms.

Confirmation Command

"SHOW RMON EVENT" on page 1190.

Example

The following example creates an event with an ID of 2, with a description of "port5_traffic," and an owner named "John" for RMON alarms:

```
awplus> enable
awplus# configure terminal
awplus(config)# rmon event 2 log description port5_traffic
owner John
```

RMON EVENT LOG TRAP

Syntax

rmon event *event_id* log trap *community_string* [description *description*] [owner *owner*]

Parameters

event_id

    Specifies the ID number of a new event. The range is 1 to 65535.

community_string

    Specifies the community string assigned the IP addresses of the network devices that are to receive the trap. You can specify just one community string. The community string is case sensitive and must already exist on the switch.

description

    Specifies a description of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed.

owner

    Specifies an owner of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed. You must enter a description to include an owner.

Mode

Global Configuration mode

Description

Use this command to create events for RMON alarms. This type of event enters a message in the event log and sends an SNMP trap when a rising or falling threshold of an alarm is crossed. The same event can be assigned to multiple alarms.

Confirmation Command

"SHOW RMON EVENT" on page 1190.

Example

This example creates an event for RMON alarms with an ID of 2, a community string of "station43a," a description of "broadcast_packets," and an owner named, "jones:"

```
awplus> enable
awplus# configure terminal
awplus(config)# rmon event 2 log trap station43a description
broadcast_packets owner jones
```

RMON EVENT TRAP

Syntax

rmon event *event_id* trap *community_string* [description *description*] [owner *owner*]

Parameters

event_id
> Specifies the ID number of a new event. The range is 1 to 65535.

community_string
> Specifies the community string assigned the IP addresses of the network devices that are to receive the trap. You can specify just one community string. The community string is case sensitive and must already exist on the switch.

description
> Specifies a description of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed.

owner
> Specifies an owner of up to 20 alphanumeric characters for the event. Spaces and special characters are not allowed. You must enter a description to include an owner.

Mode

Global Configuration mode

Description

Use this command to create events for RMON alarms. This type of event sends an SNMP trap when a rising or falling threshold of an alarm is crossed. The same event can be assigned to multiple alarms.

Confirmation Command

"SHOW RMON EVENT" on page 1190.

Example

The following example creates an event with an ID of 4, a community string of "st_west8," and a description of "router_north:"

```
awplus> enable
awplus# configure terminal
awplus(config)# rmon event 4 trap st_west8 description
router_north
```

SHOW RMON ALARM

Syntax

```
show rmon alarm
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the RMON alarms on the switch. Here is an example of the information.

```
Alarm Index = 2
    Variable etherStatsBroadcastPkts.2
    Interval 80
    Alarm Type rising and falling
    Rising Threshold = 1000
    Event Index = 5
    Falling Threshold = 100
    Event Index = 5
    Owner Agent

Alarm Index =  5
    Variable etherStatsBroadcastPkts.4
    Interval 5
    Alarm Type rising and falling
    Rising Threshold = 5000
    Event Index = 1
    Falling Threshold = 500
    Event Index = 1
    Owner Agent
```

Figure 193. SHOW RMON ALARM Command

The fields are described in Table 116.

Table 116. SHOW RMON ALARM Command

Parameter	Description
Alarm Index	The ID number of the alarm.
Variable	The MIB object the alarm is monitoring, and the ID number of the statistics group used to monitor the port and MIB object.
Interval	The polling interval in seconds.
Alarm Type	The alarm type. This is always "rising and falling," meaning the alarm has both a rising threshold and a falling threshold.
Rising Threshold	The rising threshold.
Event Index	The ID number of the event the alarm performs if the rising threshold is crossed.
Falling threshold	The falling threshold.
Event index	The ID number of the event the alarm performs if the falling threshold is crossed.
Owner	The name of the owner of the alarm. The owner is Agent if no owner was specified when the alarm was created.

Example

The following example displays the RMON alarms on the switch:

```
awplus# show rmon alarm
```

SHOW RMON EVENT

Syntax

show rmon event

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the RMON events on the switch. Here is an example of the information.

```
Event index = 2
    Description: broadcast_packets
    Event type: log & trap
    Event community name: wkst12a
    Last Time Sent = 0
    Owner: Agent
Event index = 3
    Description: port24_traffic
    Event type: log
    Event community name:
    Last Time Sent = 0
    Owner: Wilson
```

Figure 194. SHOW RMON EVENT Command

The fields are described in Table 117.

Table 117. SHOW RMON EVENT Command

Parameter	Description
Event index	The ID number of the event.
Description	The description of the event.
Event type	The event type. The types are: ❒ Log - The event enters a message in the event log. ❒ Trap - The event sends an SNMP trap.

1190

Table 117. SHOW RMON EVENT Command (Continued)

Parameter	Description
Event type (continued)	❐ Log & Trap - The event enters a message in the event log and sends an SNMP trap.
Event community name	The SNMP community string used to send SNMP traps.
Last Time Sent	The number of seconds the switch had been operating when it last sent the event trap.
Owner	The owner of the event. The owner is Agent if no owner was specified when the event was created.

Example

The following example displays the RMON events on the switch:

```
awplus# show rmon event
```

SHOW RMON HISTORY

Syntax

show rmon history

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the history groups that are assigned to the ports on the switch. Here is an example of the information.

```
History Index = 1
   Data source ifindex = 2
   Buckets requested = 50
   Buckets granted = 50
   Interval = 800
   Owner William

History Index = 4
   Data source ifindex = 7
   Buckets requested = 25
   Buckets granted = 25
   Interval = 120
   Owner Jones

History Index = 2
   Data source ifindex = 14
   Buckets requested = 50
   Buckets granted = 50
   Interval = 1800
   Owner Agent
```

Figure 195. SHOW RMON HISTORY Command

The fields are described in Table 118.

Table 118. SHOW RMON HISTORY Command

Parameter	Description
History Index	The ID number of the history group.

1192

Table 118. SHOW RMON HISTORY Command (Continued)

Parameter	Description
Data source ifindex	The port of the history group.
Buckets requested	The number of buckets that were requested in the command that created the history group.
Buckets granted	The number of buckets allocated by the switch for the history group. The value in this field will be less than the value in the buckets requested field if the switch did not have sufficient memory resources when you created the history group.
Interval	The polling interval in seconds.
Owner	The owner of the group. The owner is Agent if no owner was specified when the history group was created.

Example

The following example displays the history groups that are assigned to the ports on the switch:

```
awplus# show rmon history
```

SHOW RMON STATISTICS

Syntax

```
show rmon statistics
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the RMON statistics groups on the switch ports. Here is an example of the command.

```
Stats Index = 5
   Data source ifindex = 5
   Owner Agent

Stats Index = 16
   Data source ifindex = 16
   Owner Agent
```

Figure 196. SHOW RMON STATISTICS Command

The fields are described in Table 119.

Table 119. SHOW RMON STATISTICS Command

Parameter	Description
Stats Index	The ID number of the port statistics group.
Data source ifindex	The port number of the group.
Owner	The owner of the group. The owner is Agent if no owner was specified when the statistics group was created.

Example

```
awplus# show rmon statistics
```

1194

Chapter 73

Advanced Access Control Lists (ACLs)

This chapter describes the following topics:

Overview

Access Control Lists (ACLs) act as filters to control the ingress packets on ports. They are commonly used to restrict the types of packets ports accept to increase port security and create physical links dedicated to carrying specific types of traffic. For instance, you can configure ACLs to permit ports to accept only ingress packets that have a specific source or destination IP address.

There are two types of ACLs:

❒ Numbered IPv4 ACLs

❒ Numbered MAC ACLs

Numbered IPv4 ACLs and Numbered MAC ACLs are identified by ID numbers. The ID number range for Numbered IPv4 ACLs is 3000 to 3699. The ID number range for Numbered MAC ACLs is 4000 to 4699. In addition, Numbered IPv4 ACLs and Numbered MAC ACLs take effect immediately. You cannot assign them a date or time to begin filtering. Numbered IPv4 ACLs are only compatible with IPv4 addresses. They are not compatible with IPv6 addresses.

Filtering Criteria   All types of ACLs identify packets using filtering criteria. There are six criteria:

❒ Source and destination IP addresses

❒ ICMP source and destination IP addresses

❒ Protocol type

❒ Source and destination TCP ports

❒ Source and destination UDP ports

❒ Source and destination MAC addresses

Actions   The action defines the response to packets that match the filtering criterion of the ACL. There are three possible actions:

❐ Permit— A permit action instructs ports to forward ingress packets that match the specified traffic flow of the ACL. By default, all ingress packets are forwarded by the ports.

❐ Deny— A deny action instructs ports to discard the specified ingress packets.

❐ Copy to mirror— This action causes a port to copy all ingress packets that match the ACL to the destination port of the mirror port. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

ID Numbers   For both Numbered IPv4 ACLs and Numbered MAC ACLs, you must assign each ACL a unique ID number. There are two ID number ranges that are displayed in Table 120.

Table 120. Access Control List ID Number Ranges

Type of ACL	ID Number Range
Numbered IPv4 ACLs	3000 - 3699
Numbered MAC ACLs	4000 - 4699

How Ingress Packets are Compared Against ACLs

As stated previously, ports that do not have an ACL forward *all* ingress packets. Ports with one or more deny ACLs discard ingress packets that match the ACLs and forward all other traffic. A port that has one ACL that specifies a particular source IP address, for example, discards all ingress packets with the specified source address and forwards all other traffic. In situations where a port has more than one deny ACL, packets are discarded at the first match.

Since ports forward all ingress packets unless they have deny ACLs, permit ACLs are only necessary in situations where you want a port to forward packets that are a subset of a larger traffic flow that is blocked, for example, a port that forwards only packets having a specified destination IP address. A permit ACL specifies the packets with the intended destination IP address, and a deny ACL specifies all traffic.

When ports have both permit and deny ACLs, you must add the permit ACLs first, because packets are compared against the ACLs in the order they are added to the ports. If a permit ACL is added after a deny ACL, ports are likely to discard packets specified by the permit ACL, thus causing them to block packets you want them to forward. This concept is illustrated in the examples in this chapter.

Guidelines Here are the ACL guidelines:

❒ An ACL can have a permit, deny, or copy-to-mirror action. The permit action allows ports to forward ingress packets of the designated traffic flow while the deny action causes ports to discard packets. The copy-to-mirror action causes a port to copy all ingress packets that match the ACL to the destination port of the mirror port.

❒ A port can have more than one ACL.

❒ An ACL can be assigned to more than one port.

❒ You can only assign the same ACL to the same port one time.

❒ ACLs filter ingress packets on ports, but they do not filter egress packets. As a result, you must apply ACLs to the ingress ports of the designated traffic flows.

❒ ACLs for static port trunks or LACP trunks must be assigned to the individual ports of the trunks.

❒ Because ports, by default, forward all ingress packets, permit ACLs are only required in circumstances where you want ports to forward packets that are subsets of larger packet flows that are blocked by deny ACLs.

❒ A port that has more than one ACL checks the ingress packets in the order in which the ACLs are added, and forwards or discards packets at the first match. As a result, if a port has both permit and deny ACLs, add the permit ACLs *before* the deny ACLs. Otherwise, a port is likely to discard packets you want it to forward.

❒ Ports can have ACLs with different filtering criteria. For example, a port may have ACLs that filter on a source IP address and a UDP port.

1198

Creating ACLs

This section provides examples of how to create all of the ACL types. See the following:

❐ "Creating Numbered IPv4 ACLs" on page 1199

❐ "Creating Numbered MAC ACLs" on page 1211

For descriptions of the commands mentioned in these procedures, refer to Chapter 74, "ACL Commands" on page 1229.

Creating Numbered IPv4 ACLs

Depending on the type of filter that you want to create, there are five commands for creating Numbered IPv4 ACLs. These commands are listed in Table 121. All of the commands for creating Numbered IPv4 ACLs begin with "ACCESS-LIST" and are found in the Global Configuration mode.

For examples of the commands listed in Table 121, see the following:

❐ "Numbered IPv4 ACL with IP Packets Examples" on page 1200

❐ "Numbered IPv4 ACL with ICMP Packets Example" on page 1204

❐ "Numbered IPv4 ACL with Protocol Packets Example" on page 1206

❐ "Numbered IPv4 ACL with TCP Port Packets Example" on page 1207

❐ "Numbered IPv4 ACL with UDP Port Packets Example" on page 1209

Table 121. ACCESS-LIST Commands for Creating Numbered IPv4 ACLs

To Do This Task	Use This Command
Create Numbered IPv4 ACLs for source and destination IPv4 addresses.	`ACCESS-LIST` *id_number action* IP *src_ipaddress dst_ipaddress* [VLAN *vid*]
Create Numbered IPv4 ACLs for ICMP packets.	`ACCESS-LIST` *id_number action* ICMP *src_ipaddress dst_ipaddress* [VLAN *vid*]
Create Numbered IPv4 ACLs for packets of specified protocols.	`ACCESS-LIST` *id_number action* PROTO *protocol_number src_ipaddress dst_ipaddress* [vlan *vid*]
Create Numbered IPv4 ACLs that filter ingress packets based on TCP port numbers.	`ACCESS-LIST` *id_number action* TCP *src_ipaddress* EQ|LT|GT|NE|RANGE *src_tcp_port dst_ipaddress* EQ|LT|GT|NE|RANGE *dst_tcp_port* [VLAN *vid*]
Create Numbered IPv4 ACLs that filter ingress packets based on UDP port numbers.	`ACCESS-LIST` *id_number action* UDP *src_ipaddress* EQ|LT|GT|NE|RANGE *src_udp_port dst_ipaddress* EQ|LT|GT|NE|RANGE *dst_udp_port* [VLAN *vid*]

Numbered IPv4 ACL with IP Packets Examples

This is the command format for creating ACLs that filter IP packets based on source and destination IPv4 addresses:

access-list *id_number action* ip *src_ipaddress dst_ipaddress* [vlan *vid*]

The ID_NUMBER parameter assigns the ACL a unique ID number in the range of 3000 to 3699. Within this range, you can number ACLs in any order.

The ACTION parameter specifies the action that the port performs on packets matching the filtering criteria of the ACL. Here are the possible actions:

- permit— Forwards all ingress packets that match the ACL. Ports, by default, accept all ingress packets. Consequently, a permit ACL is only necessary when you want a port to forward a subset of packets that are otherwise discarded.

- deny— Discards all ingress packets that match the ACL.

- copy-to-mirror— Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used together with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

The SRC_IPADDRESS and DST_IPADDRESS parameters specify the source and destination IPv4 addresses. Choose from the following options:

- any— Matches any IP address.

- *ipaddress/mask*— Matches packets that have an IP address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of "24" for the first twenty-four bits of the network portion of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24."

❒ host *ipaddress*— Matches packets with a specified IPv4 address and is an alternative to the IPADRESS/MASK variable for addresses of end nodes. The HOST keyword indicates that the IPv4 address is assigned to a specific end node and that no mask is required.

The *VLAN* parameter determines if an ACL filters VLANs. You use the parameter to specify the VID. You can specify one VID per command. If you omit this parameter, the ACL applies to *all* traffic. In other words, no filtering is done by the ACL based on the VLAN.

The following tables provide several examples of the command. In Table 122, a Numbered IPv4 ACL is created with an ID number of 3097, that blocks all untagged ingress packets with the specified destination address of 149.107.22.0/24:

Table 122. Blocking Ingress Packets Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# access-list 3097 deny ip any 149.107.22.0/24	Create the deny ACL with the ACCESS-LIST IP command.

The example in Table 123 creates two Numbered IPv4 ACLs that block all traffic with specified subnets 149.87.201.0/24 and 149.87.202.0/24.

Table 123. Blocking Traffic with Two IPv4 Addresses

Command	Description
awplus> enable	Enters the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enters the Global Configuration mode.
awplus(config)# access-list 3104 deny ip 149.87.201.0/24 any	Creates the deny ACL for the packets from the 149.87.201.0/24 subnet.
awplus(config)# access-list 3105 deny ip 149.87.202.0/24 any	Creates the deny ACL for the packets from the 149.87.202.0/24 subnet.

If you want a port to forward a subset of packets of a more-specific traffic flow, you have to create a permit ACL for the permitted packets and a

1201

deny ACL for the denied traffic flow. This is illustrated in the example in Table 124 in which port 15 is configured to forward only ingress packets from the 149.55.65.0/24 subnet and to discard all other traffic. The permit ACL, which has the ID number 3015, specifies the packets from the permitted subnet, while the deny ACL, with the ID number 3011, specifies all traffic.

Note
In the example, the permit ACL is added to the port *before* the deny ACL. This is important because packets are compared against the ACLs in the order in which the ACLs are added to the port. If the deny ACL is added first, the port blocks all traffic, even the traffic specified by the permit ACL.

Table 124. Creating a Permit ACL Followed by a Deny ACL Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# access-list 3015 permit ip 149.55.65.0/24 any`	Create the permit ACL with the ACCESS-LIST command.
`awplus(config)# access-list 3011 deny ip any any`	Create the deny ACL.
`awplus(config)# interface port1.0.15`	Move to the Port Interface mode for port 15.
`awplus(config_if)# access-group 3015` `awplus(config_if)# access-group 3011`	Add the two ACLs to the port with the ACCESS-GROUP command, being sure to add the permit ACL first so that ingress packets are compared against it first.
`awplus(config_if)# end`	Return to the Privileged Exec mode.
`awplus# show access-list`	Confirm the configuration of the ACLs.
`awplus# show interface port1.0.15 access-group`	Confirm that the ACLs have been added to the port.

For another example of permit ACLs, see Table 125 on page 1203. In this example, ports 21 and 22 forward traffic from three specified network devices and discard all other ingress traffic. The allowed traffic is specified with three permit ACLs.

> **Note**
> The permit ACLS are added to the ports before the deny ACL to ensure that packets are compared against them first.

Table 125. Permit ACLs IPv4 Packets Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.

`awplus(config)# access-list 3021 permit ip 149.124.242.52/32 any`
 	
`awplus(config)# access-list 3022 permit ip 149.124.242.53/32 any`
 	
`awplus(config)# access-list 3023 permit ip 149.124.242.54/32 any`
	Create the three permit ACLs with the ACCESS-LIST command.

`awplus(config)# access-list 3018 deny ip any any`	Create the deny ACL.
`awplus(config)# interface port1.0.21, port1.0.22`	Move to the Port Interface mode for ports 21 and 22.

`awplus(config_if)# access-group 3021`
`awplus(config_if)# access-group 3022`
`awplus(config_if)# access-group 3023`
`awplus(config_if)# access-group 3018`
	Add the ACLs to the port with the ACCESS-GROUP command, being sure to add the permit ACLs first so that ingress packets are compared against them first.

`awplus(config_if)# end`	Return to the Privileged Exec mode.
`awplus# show access-list`	Confirm the configuration of the ACLs.
`awplus# show interface port1.0.21,port1.0.22 access-group`	Confirm that the ACLs have been added to the port.

Here is an example of an ACL that filters tagged packets. See Table 126. It blocks all tagged packets with the VID 14 from ports 5 and 6. The ACL is assigned an ID number of 3122:

Table 126. ACL Filters Tagged IPv4 Packets Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# access-list 3122 deny ip any any vlan 14`	Create the deny ACL with the ACCESS-LIST IP command.
`awplus(config)# interface port1.0.5, port1.0.6`	Move to the Port Interface mode for ports 5 and 6.
`awplus(config_if)# access-group 3122`	Apply the ACL to the port with the ACCESS-GROUP command.
`awplus(config_if)# end`	Return to the Privileged Exec mode.
`awplus# show access-list`	Confirm the configuration of the ACL.
`awplus# show interface port1.0.5,port1.0.6 access-group`	Confirm that the ACL has been added to the port.

Numbered IPv4 ACL with ICMP Packets Example

This is the command format for creating Numbered IPv4 ACLs that filter ICMP packets based on source and destination IPv4 addresses:

access-list *id_number action* icmp *src_ipaddress dst_ipaddress* [vlan *vid*]

The ID_NUMBER parameter assigns the ACL a unique ID number in the range of 3000 to 3699. Within this range, you can number ACLs in any order.

The ACTION parameter specifies the action that the port performs on packets matching the filtering criteria of the ACL. Here are the possible actions:

❐ permit— Forwards all ingress packets that match the ACL. Ports, by default, accept all ingress packets. Consequently, a permit ACL

is only necessary when you want a port to forward a subset of packets that are otherwise discarded.

❐ deny— Discards all ingress packets that match the ACL.

❐ copy-to-mirror— Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used together with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

The SRC_IPADDRESS and DST_IPADDRESS parameters specify the source and destination IPv4 addresses. Choose from the following options:

❐ any— Matches any IPv4 address.

❐ *ipaddress/mask*— Matches packets that have an IPv4 address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of "24" for the first twenty-four bits of the network portion of the address. The IPv4 address and the mask are separated by a slash (/); for example, "149.11.11.0/24."

❐ host *ipaddress*— Matches packets with a specified IPv4 address and is an alternative to the IPADRESS/MASK variable for addresses of end nodes. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

The *VLAN* parameter determines if an ACL filters VLANs. You use the parameter to specify the VID. You can specify one VID per command. If you omit this parameter, the ACL applies to *all* traffic. In other words, no filtering is done by the ACL based on the VLAN.

In the following example, a Numbered IPv4 ACL is created with an ID number of 3000, that blocks all untagged ingress ICMP packets with a source address of 192.168.1.10/32:

Table 127. Numbered IPv4 ACL with ICMP Packets Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# access-list 3000 deny icmp host 192.168.1.10 any	Creates a Numbered IPv4 ACL with an ID of 3000 that denies ICMP packets from the host source address of 192.168.1.10.

Numbered IPv4 ACL with Protocol Packets Example

This is the command format for creating Numbered IPv4 ACLs that filter packets of the specified protocol based on source and destination IPv4 addresses:

```
access-list id_number action proto protocol_number
src_ipaddress dst_ipaddress [vlan vid]
```

The ID_NUMBER parameter assigns the ACL a unique ID number in the range of 3000 to 3699. Within this range, you can number ACLs in any order.

The ACTION parameter specifies the action that the port performs on packets matching the filtering criteria of the ACL. Here are the possible actions:

- permit— Forwards all ingress packets that match the ACL. Ports, by default, accept all ingress packets. Consequently, a permit ACL is only necessary when you want a port to forward a subset of packets that are otherwise discarded.

- deny— Discards all ingress packets that match the ACL.

- copy-to-mirror— Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used together with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

The *protocol_number* parameter specifies a protocol number. You can specify one protocol number per command. Refer to Table 144, "Protocol Numbers" on page 1246 for the list of protocol numbers.

The SRC_IPADDRESS and DST_IPADDRESS parameters specify the source and destination IP addresses. Choose from the following options:

- any— Matches any IPv4 address.

- *ipaddress/mask*— Matches packets that have an IPv4 address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of "24" for the first twenty-four bits of the network portion of the address. The IPv4 address and the mask are separated by a slash (/); for example, "149.11.11.0/24."

- host *ipaddress*— Matches packets with a specified IPv4 address and is an alternative to the IPADRESS/MASK variable for addresses of end nodes. The HOST keyword indicates that the IPv4 address is assigned to a specific end node and that no mask is required.

1206

The *VLAN* parameter determines if an ACL filters VLANs. You use the parameter to specify the VID. You can specify one VID per command. If you omit this parameter, the ACL applies to *all* traffic. In other words, no filtering is done by the ACL based on the VLAN.

This example creates a deny access list to ports 5 and 6 so that they discard all tagged ingress packets that contain protocol 17, a VID of 12, and originate from the 152.12.45.0 subnet. The access list is assigned the ID number 3011:

Table 128. Numbered IPv4 ACL with Protocol Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# access-list 3011 deny proto 17 152.12.45.0/24 any vlan 12	Create a Numbered IPv4 ACL with an ID of 3011 that denies protocol 17 packets and VLAN ID 12 from the host source address of 152.12.45.0/24 subnet.

Numbered IPv4 ACL with TCP Port Packets Example

This is the command format for creating Numbered IPv4 ACLs that filter packets from TCP ports based on source and destination IPv4 addresses:

access-list *id_number action* tcp *src_ipaddress* eq|lt|gt|ne|range *src_tcp_port dst_ipaddress* eq|lt|gt|ne|range *dst_tcp_port* [vlan *vid*]

The ID_NUMBER parameter assigns the ACL a unique ID number in the range of 3000 to 3699. Within this range, you can number ACLs in any order.

The ACTION parameter specifies the action that the port performs on packets matching the filtering criteria of the ACL. Here are the possible actions:

❒ permit— Forwards all ingress packets that match the ACL. Ports, by default, accept all ingress packets. Consequently, a permit ACL is only necessary when you want a port to forward a subset of packets that are otherwise discarded.

❒ deny— Discards all ingress packets that match the ACL.

❒ copy-to-mirror— Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used together with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

The SRC_IPADDRESS and DST_IPADDRESS parameters specify the source and destination IPv4 addresses. Choose from the following options:

❏ any— Matches any IPv4 address.

❏ *ipaddress/mask*— Matches packets that have an IPv4 address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of "24" for first the twenty-four bits of the network portion of the address. The IPv4 address and the mask are separated by a slash (/); for example, "149.11.11.0/24."

❏ host *ipaddress*— Matches packets with a specified IPv4 address and is an alternative to the IPADRESS/MASK variable for addresses of end nodes. The HOST keyword indicates that the IPv4 address is assigned to a specific end node and that no mask is required.

The *eq* parameter matches packets that are equal to the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

The *lt* parameter matches packets that are less than the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

The *gt* parameter matches packets that are greater than the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

The *ne* parameter matches packets that are not equal to the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

The *range* parameter matches packets with TCP port numbers within the range. Separate the numbers of the range by a space. For instance:

range 4 10

The *src_tcp_port* parameter specifies the source TCP port number. The range is 0 to 65535. Omit this parameter to match any TCP port number within the 0 to 65535 range.

The *dst_tcp_port* parameter specifies the destination TCP port number. The range is 0 to 65535. Omit this parameter to match any TCP port number within the 0 to 65535 range.

The *VLAN* parameter determines if an ACL filters VLANs. You use the parameter to specify the VID. You can specify one VID per command. If you omit this parameter, the ACL applies to all traffic. In other words, no filtering is done by the ACL based on the VLAN.

The following example configures two Numbered IPv4 ACLs. ACL 3017 permits packets from TCP port 67 to 87 on IPv4 addresses 154.11.234.0/24 to 154.11.235.0/24. ACL 3005 denies packets from TCP ports 67 through 87 to any IPv4 address. This example requires a permit ACL because the permitted traffic is a subset of all TCP packets on the port:

Table 129. Numbered IPv4 ACL with TCP Port Packets Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# access-list 3017 permit tcp 154.11.234.0/24 range 67 87 154.11.235.0/24 range 67 87`	Define ACL 3017 to permit packets from TCP port 67 to 87 on IPv4 addresses 154.11.234.0/24 to 154.11.235.0/24.
`awplus(config)# access-list 3005 deny tcp any any range 67 87`	Define ACL 3005 to deny packets from TCP ports 67 through 87 to any IPv4 address.
`awplus(config)# interface port1.0.21`	Move to the Port Interface mode for port 21.
`awplus(config_if)# access-group 3017`	Apply ACL 3017 to the port with the ACCESS-GROUP command.
`awplus(config_if)# access-group 3005`	Apply ACL 3005 to the port with the ACCESS-GROUP command.

Numbered IPv4 ACL with UDP Port Packets Example

```
access-list id_number action udp src_ipaddress
eq|lt|gt|ne|range src_udp_port dst_ipaddress
eq|lt|gt|ne|range dst_udp_port vlan vid
```

The ID_NUMBER parameter assigns the ACL a unique ID number in the range of 3000 to 3699. Within this range, you can number ACLs in any order.

The ACTION parameter specifies the action that the port performs on packets matching the filtering criteria of the ACL. Here are the possible actions:

❒ permit— Forwards all ingress packets that match the ACL. Ports, by default, accept all ingress packets. Consequently, a permit ACL is only necessary when you want a port to forward a subset of packets that are otherwise discarded.

❒ deny— Discards all ingress packets that match the ACL.

❒ copy-to-mirror— Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used

1209

together with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

The SRC_IPADDRESS and DST_IPADDRESS parameters specify the source and destination IPv4 addresses. Choose from the following options:

❐ any— Matches any IPv4 address.

❐ *ipaddress/mask*— Matches packets that have an IPv4 address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of "24" for the first twenty-four bits of the network portion of the address. The IPv4 address and the mask are separated by a slash (/); for example, "149.11.11.0/24."

❐ host *ipaddress*— Matches packets with a specified IPv4 address and is an alternative to the IPADRESS/MASK variable for addresses of end nodes. The HOST keyword indicates that the IPv4 address is assigned to a specific end node and that no mask is required.

The *eq* parameter matches packets that are equal to the UDP port number specified by the SRC_UDP _PORT or DST_UDP _PORT parameter.

The *lt* parameter matches packets that are less than the UDP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

The *gt* parameter matches packets that are greater than the UDP port number specified by the SRC_UDP _PORT or DST_UDP _PORT parameter.

The *ne* parameter matches packets that are not equal to the UDP port number specified by the SRC_UDP _PORT or DST_UDP _PORT parameter.

The *range* parameter matches packets with UDP port numbers within the range. Separate the numbers of the range by a space. For instance:

range 4 10

The *src_udp_port* parameter specifies the source UDP port number. The range is 0 to 65535. Omit this parameter to match any UDP port number within the 0 to 65535 range.

The *dst_udp_port* parameter specifies the destination UDP port number. The range is 0 to 65535. Omit this parameter to match any UDP port number within the 0 to 65535 range.

1210

The *VLAN* parameter determines if an ACL filters VLANs. You use the parameter to specify the VID. You can specify one VID per command. If you omit this parameter, the ACL applies to *all* traffic. In other words, no filtering is done by the ACL based on the VLAN.

The following example configures two ACLs. When they are applied in combination on port 21, they forward tagged packets to UDP source and destination ports in the range of 67 to 87 only if they are from the 154.11.234.0 network and are going to the 154.11.235.0 network, and have the VID, 20. The Numbered IPv4 ACL with UDP port example requires a permit ACL because the permitted traffic is a subset of all UDP packets on the port:

Table 130. Numbered IPv4 ACL with UDP Port Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# access-list 3119 permit udp 154.11.234.0/24 range 67 87 154.11.235.0/24 range 67 87 vlan 20`	Define ACL 3119 to permit packets from UDP ports 67 through 87 on IP addresses 154.11.234.0/24 and 154.11.234.0/24, and VLAN with a VID of 20.
`awplus(config)# access-list 3005 deny udp any any range 67 87`	Define ACL 3005 to deny packets from UDP ports 67 through 87 from any source or destination IPv4 address.

Creating Numbered MAC ACLs

There is one command to create Numbered MAC ACLs. The following command creates Numbered MAC ACLs that filter source and destination MAC addresses. Here is the format:

`ACCESS-LIST` *id_number action src_mac_address*|`ANY` *src_mac_mask dst_mac_address*|`ANY` *dst_mac_mask*

The *id_number* parameter specifies the ID number for the new ACL. The range is 4000 to 4699.

The ACTION parameter specifies the action that the port performs on packets matching the filtering criteria of the ACL. Here are the possible actions:

❑ permit— Forwards all ingress packets that match the ACL. Ports, by default, accept all ingress packets. Consequently, a permit ACL is only necessary when you want a port to forward a subset of packets that are otherwise discarded.

❑ deny— Discards all ingress packets that match the ACL.

1211

❏ copy-to-mirror— Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used together with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

The *src_mac_address* parameter specifies the source MAC address of the ingress packets. Here are the possible options:

❏ *src_mac_address*— Specifies the source MAC address of the packets. The address must be entered in hexadecimal in one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

❏ any— Matches any source MAC address.

The *src_mac_mask* parameter specifies the source MAC address mask. The mask must be entered in one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

The "x" variable can be either "0" or "F". Use a "0" mask to indicate the parts of the MAC address the ACL is to filter. Use an "F" mask for parts of the MAC address the ACL should ignore.

Note
Do not include a mask if you specified ANY as the source MAC address.

The *dst_mac_address* parameter specifies the destination MAC address of the ingress packets. Here are the possible options:

❏ *dst_mac_address*— Specifies the destination MAC address of the packets. The address must be entered in hexadecimal in one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

❏ any— Matches any destination MAC address.

The *dst_mac_mask* parameter specifies the destination MAC address mask. The mask must be entered in one of the following formats: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

The "x" variable can be either "0" or "F". Use a "0" mask for parts of the MAC address the ACL is to filter. Use an "F" mask for parts of the MAC address the ACL should ignore.

```
awplus(config)# access-list 4000 deny any
00:ao:d2:01:02:04 00:00:00:00:00:00 any vlan 20
```

1212

The example in Table 131 configures port 19 to reject packets containing destination MAC addresses starting with A4:54:86:12:

Table 131. Numbered MAC ACL Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# access-list 4102 deny any a4:54:86:12:00:00 00:00:00:00:ff:ff	Define ACL 4012 to deny any frame with the destination MAC address that starts with a4:54:86:12.
awplus(config)# interface port1.0.19	Access the Port Interface mode for port 19.
awplus(config_if)# mac access-group 4102	Apply the ACL to the port.

Assigning ACLs to Ports

Before you can assign an ACL to a port, you must first create an ACL. The command that you use to assign an ACL to a port depends on which type of ACL you have created. See the following sections:

❒ "Assigning Numbered IPv4 ACLs to a Port" on page 1214

❒ "Assigning MAC Address ACLs to a Port" on page 1215

> **Note**
> In situations where ports have both permit and deny ACLs, you must assign the permit ACLs to a port *first* because ingress packets are compared against the ACLs in the order in which they are added to the ports. If you add the deny ACLs first, the ports may block packets you want them to forward.

Assigning Numbered IPv4 ACLs to a Port

To assign a Numbered IPv4 ACL to a port on the switch, use the ACCESS-GROUP command in the Port Interface mode. Using this command, you can add one Numbered IPv4 ACL to a port or several ports. The ACL must exist on the switch. Here is the format of the command:

`access-group` *id_number*

For more information about this command, see "ACCESS-GROUP" on page 1233.

In this example, ports 12 and 13 are assigned an ACL, ID number 3075, that blocks all untagged ingress packets with a destination address in the 149.107.22.0 subnet. See Table 132.

Table 132. Assigning Numbered IPv4 ACLs

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# access-list 3075 deny ip any 149.107.22.0/24`	Create the deny ACL.
`awplus(config)# interface port1.0.12,port1.0.13`	Enter the Port Interface mode for ports 12 and 13.
`awplus(config_if)# access-group 3075`	Apply the ACL to the ports with the ACCESS-GROUP command.

Assigning MAC Address ACLs to a Port

To assign a MAC ACL to a port on the switch, use the MAC ACCESS-GROUP command in the Port Interface mode. Using this command, you can add one MAC ACL to a port or several ports. The ACL must exist on the switch. Here is the format of the command:

`mac access-group` *id_number*

For more information about this command, see "MAC ACCESS-GROUP" on page 1258.

This example creates two MAC ACLs with ID numbers of 4025 and 4055. ACL 4025 permits only packets that have source MAC addresses starting with "45:2A:B5:". ACL 4055 denies all other MAC addresses. Then assign both ACLs to port 7:

Table 133. Assigning MAC Address ACLs Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# access-list 4025 permit 45:2a:b5:00:00:00 00:00:00:ff:ff:ff any`	Create the permit ACL.
`awplus(config)# access-list 4055 deny any any`	Create the deny ACL.

1215

Table 133. Assigning MAC Address ACLs Example (Continued)

Command	Description
awplus(config)# interface port1.0.7	Move to the Port Interface mode for port 7.
awplus(config_if)# mac access-group 4025	Apply the ACL to the port with the ACCESS-GROUP command.
awplus(config_if)# mac access-group 4055	Apply the ACL to the port with the ACCESS-GROUP command.

Removing ACLs from Ports

The command that you use to remove an ACL from a port depends on which type of ACL you have created. See the following sections:

❐ "Removing Numbered IPv4 ACLs" on page 1217

❐ "Removing MAC Address ACLs" on page 1217

Removing Numbered IPv4 ACLs

To remove Numbered IPv4 ACLs from ports so that the ports stop filtering traffic, use the NO ACCESS-GROUP command in the Port Interface mode. The command has the following format:

no access-group *id_number*

For more information about this command, see "ACCESS-GROUP" on page 1233.

With this command, you can remove one ACL at a time. See Table 134. The following example removes an ACL with an ID number of 3082 from port 15:

Table 134. Removing Numbered IP ACLs Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface port1.0.15	Enter the Port Interface mode for port 15.
awplus(config_if)# no access-group 3082	Remove ACL 3082 from port 15.

Removing MAC Address ACLs

To remove a MAC ACL from a port on the switch, use the NO MAC ACCESS-GROUP command in the Port Interface mode. Here is the format of the command:

no mac access-group *id_number*

For more information about this command, see "NO ACCESS-LIST" on page 1259.

This example removes a MAC ACL with an ID number of 4037 from port 5:

Table 135. Removing MAC Address ACLs Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface port1.0.5`	Enter the Port Interface mode for port 5.
`awplus(config_if)# no mac access-group 4037`	Remove MAC ACL 4037 from port 5.

Restricting Remote Access

You can access the switch remotely through the VTY lines. Unrestricted remote access is available through Telnet and the Web interfaces as well as through the SNMP and SSH protocols by default. The ACCESS-LIST command allows you to control remote access to the switch through VTY lines. First you create an ACL and then you use the ACCESS-LIST command to make the assignment to the VTY lines. This command is similar to the ACCESS-GROUP command which allows you to assign an ACL to a port.

You can add one ACL per command. Also, you can add multiple ACLs to the VTY lines as shown in the examples that follow.

Allied Telesis recommends specifying all ten of the VTY lines with the ACCESS-LIST command because the switch assigns VTY lines randomly.

For procedures that use the ACCESS-LIST command, see the following:

❒ "Assigning Numbered IP ACLs to VTY Lines" on page 1219
❒ "Assigning MAC ACLs to VTY Lines" on page 1220

"Assigning Named IPv4 and IPv6 ACLs to VTY Lines" on page 1221

Assigning Numbered IP ACLs to VTY Lines

The following example creates two Numbered IP ACLs. The first ACL created, with an ID of 3000, permits IP address 10.0.0.3 full access to the switch. The second ACL created, with an ID of 3001, denies all IP addresses access to the switch. Both ACLs are assigned to all ten VTY lines with the ACCESS-CLASS command in the order that the ACLs were created. The result of this example is that only IP address 10.0.0.3 has remote access to the switch. See Table 136.

Table 136. Assigning Numbered IP ACLs to VTY Lines Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# interface vlan10`	Enter the Port Interface mode for VLAN 10.
`awplus(config_if)# ip address 10.0.0.20/24`	Assign VLAN 10 an IP address and subnet mask of 10.0.0.20/24.
`awplus(config_if)# q`	Quit the Port Interface mode.

Table 136. Assigning Numbered IP ACLs to VTY Lines Example (Continued)

Command	Description
awplus(config)# access-list 3000 permit ip host 10.0.0.3 host 10.0.0.20	Creates an ACL with an ID number of 3000 that allows IP address 10.0.0.3 full access to the switch.
awplus(config)# access-list 3001 deny ip any host 10.0.0.20	Creates an ACL with an ID number of 3001 that denies all IP addresses access to the switch.
awplus(config)# line vty 0 9	Access the LINE VTY mode for lines 0 through 9.
awplus(config-line)# access-class 3000	Assigns ACL 3000 to VTY lines 0 through 9.
awplus(config-line)# access-class 3001	Assigns ACL 3001 to VTY lines 0 through 9.

Assigning MAC ACLs to VTY Lines

This example creates two MAC ACLs. The first MAC ACL created, with an ID of 4000, permits IP address 10.0.0.5 full access to the switch. The second MAC ACL has an ID of 4001 and denies all IP addresses access to the switch. Both MAC ACLs are assigned to all ten VTY lines with the ACCESS-CLASS command in the order that the ACLs were created. The result of this example is that only IP address 10.0.0.5 has remote access to the switch. See Table 137.

Note
MAC ACLs are specified with an ACL ID number within the 4000 to 4699 range.

Table 137. Assigning MAC ACLs to VTY Lines Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface vlan10	Enter the Port Interface mode for VLAN 10.
awplus(config_if)# ip address 10.0.0.20/24	Assign VLAN 10 an IP address and subnet mask of 10.0.0.20/24.
awplus(config_if)# q	Quit the Port Interface mode.

Table 137. Assigning MAC ACLs to VTY Lines Example (Continued)

Command	Description
awplus(config)# mac access-list 4000 permit ip host 10.0.0.5 host 10.0.0.20	Creates an ACL with an ID number of 4000 that allows IP address 10.0.0.5 full access to the switch.
awplus(config)# mac access-list 4001 deny ip any host 10.0.0.20	Creates an ACL with an ID number of 4001 that denies all IP addresses access to the switch.
awplus(config)# line vty 0 9	Access the LINE VTY mode for lines 0 through 9.
awplus(config-line)# access-class 4000	Assigns ACL 4000 to VTY lines 0 through 9.
awplus(config-line)# access-class 4001	Assigns ACL 4001 to VTY lines 0 through 9.

Assigning Named IPv4 and IPv6 ACLs to VTY Lines

When you create a named IPv4 or IPv6 ACL, you enter the commands in the IP ACL command mode or the Configuration IPv6 ACL command mode, respectively. The following examples show how to assign IPv4 and IPv6 ACLs to VTY lines. See the following:

❑ "Assigning Named IPv4 ACLs to VTY Lines" on page 1221

❑ "Assigning Named IPv6 ACLs to VTY Lines" on page 1222

Assigning Named IPv4 ACLs to VTY Lines

This example creates a Named IPv4 ACL, called "deny-all-but-one," that grants IP address 10.0.0.7 full access to the switch and then denies all IP addresses access to the switch. Then deny-all-but-one is assigned to all ten VTY lines with the ACCESS-CLASS command. The result of this example is that only IP address 10.0.0.7 has remote access to the switch. See Table 138.

Table 138. Assigning Named IPv4 ACLs to VTY Lines Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface vlan10	Enter the Port Interface mode for VLAN 10.

Table 138. Assigning Named IPv4 ACLs to VTY Lines Example (Continued)

Command	Description
awplus(config_if)# ip address 10.0.0.20/24	Assign VLAN 10 an IP address and subnet mask of 10.0.0.20/24.
awplus(config_if)# q	Quit the Port Interface mode.
awplus(config)# ip access-list deny-all-but-one	Creates a Named IPv4 ACL call "deny-all-but-one and enters the IP ACL command mode.
awplus(config-ip-acl)# permit ip host 10.0.0.7 host 10.0.0.20	Allows IP address 10.0.0.7 full access to the switch.
awplus(config-ip-acl)# deny ip any host 10.0.0.20	Denies access all IP addresses access to the switch.
awplus(config-ip-acl)# exit	Exit the IP ACL command mode.
awplus(config)# line vty 0 9	Access the LINE VTY mode for lines 0 through 9.
awplus(config-line)# access-class deny-all-but-one	Assigns deny-all-but-one to VTY lines 0 through 9.

Assigning Named IPv6 ACLs to VTY Lines

This example creates a Named IPv6 ACL, called "deny-all-but-one-ipv6," that grants IPv6 address 2001:odb8::a2/64 full access to the switch and then denies all IP addresses access to the switch. Then deny-all-but-one-ipv6 is assigned to all ten VTY lines with the ACCESS-CLASS command. The result of this example is that only IP address 2001:odb8::a5/64 has remote access to the switch. See Table 139.

Table 139. Assigning Named IPv4 ACLs to VTY Lines Example

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# interface vlan10	Enter the Port Interface mode for VLAN 10.
awplus(config_if)# ip address 2001:odb8::a5/64	Assign VLAN 10 an IPv6 address and subnet mask of 2001:odb8::a5/64.
awplus(config_if)# q	Quit the Port Interface mode.

Table 139. Assigning Named IPv4 ACLs to VTY Lines Example (Continued)

Command	Description
awplus(config)# ipv6 access-list deny-all-but-one	Creates a Named IPv6 ACL call "deny-all-but-one-ipv6" and enters the Configuration IPv6 ACL command mode.
awplus(config-ipv6-acl)# permit ip host 2001:odb8::a2/64 host 2001:odb8::a5/64	Allows IPv6 address and subnet mask 2001:odb8::a2/64 full access to the switch.
awplus(config-ipv6-acl)# deny ip any host 2001:odb8::a5/64	Denies access all IP addresses access to the switch.
awplus(config-ipv6-acl)# exit	Exit the Configuration IPv6 ACL mode command mode.
awplus(config)# line vty 0 9	Access the LINE VTY mode for lines 0 through 9.
awplus(config-line)# access-class deny-all-but-one	Assigns deny-all-but-one to VTY lines 0 through 9.

Unrestricting Remote Access

To restore unrestricted remove access to VTY lines through the Telnet and Web GUI interfaces as well as through SSH and SNMP protocols, use the NO ACCESS-LIST command. In the following example, Numbered IP ACLs 3000 and 3001 are removed from VTY Lines 0 through 9. See Table 140.

Table 140. Removing Numbered IP ACLs from VTY Lines Example

Command	Description
`awplus> enable`	Enter the Privileged Executive mode from the User Executive mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# line vty 0 9`	Access the LINE VTY mode for lines 0 through 9.
`awplus(config-line)# no access-class 3000`	Removes ACL 3000 from VTY lines 0 through 9.
`awplus(config-line)# no access-class 3001`	Removes ACL 3001 from VTY lines 0 through 9.

Deleting Numbered IP and MAC Address ACLs

The NO ACCESS-LIST command in the Global Configuration mode is the command that deletes Numbered IP and MAC Address ACLs from the switch. It has the following format:

no access-list *id_number*

You can delete one ACL at a time with this command. Before you can delete ACLs that are assigned to ports, you must remove them from their port assignments. For instructions, see "Removing Numbered IPv4 ACLs" on page 1217 and "Removing MAC Address ACLs" on page 1217.

The following example deletes Numbered IP ACLs with ID numbers 3018 and 3019 from the switch:

Table 141. Deleting Numbered IP ACLs Example 1

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# no access-list 3018	Remove Numbered IP ACL with ID number 3018 from the switch.
awplus(config)# no access-list 3019	Remove Numbered IP ACL with ID number 3019 from the switch.

The following example deletes a MAC ACL with ID number 4415 from the switch:

Table 142. Deleting Numbered IP ACLs Example 2

Command	Description
awplus> enable	Enter the Privileged Executive mode from the User Executive mode.
awplus# configure terminal	Enter the Global Configuration mode.
awplus(config)# no access-list 4415	Remove Numbered IP ACL with ID number 4415 from the switch.

Displaying the ACLs

There are several ways of displaying information about ACLs on the switch. You can use one command to display a list the Numbered IP IP ACLs. In addition, you can display the port assignments of all the ACLs and the ACLs assigned to VTY lines. See the following:

❐ "Displaying IPv4 ACLs" on page 1226

❐ "Displaying IP ACL Port Assignments" on page 1226

❐ "Displaying ACLs Assigned to VTY Lines" on page 1227

Displaying IPv4 ACLs

To display the Numbered IPv4 and Named IPv4 ACLs, use the SHOW ACCESS-LIST command in the Privileged Exec mode. Here is the command syntax followed by an example display.

```
awplus# show access-list
```

```
IP access-list 3000
    permit icmp any any
IP access-list 3104
    deny 149.87.201.1 mask 255.255.255.0 any
MAC access-list 4400
    permit any any
IP access-list icmppermit
    ICMP permit an any time-range daily
IP access-list denytcp
    TCP deny 149.55.65.0 mask 255.255.255.0 any time-range NONE

Total number of access-lists= 5
```

Figure 197. SHOW ACCESS-LIST Command

As you can see from the example, the SHOW ACCESS-LIST command does not display which, if any, ports the ACLs are assigned to. To display that information, use the SHOW INTERFACE ACCESS-GROUP command. See "Displaying IP ACL Port Assignments," next.

Displaying IP ACL Port Assignments

To display the IP ACL port assignments for both IPv4 and IPv6 ACLs, use the SHOW INTERFACE ACCESS-GROUP command in the Privileged Exec mode. Here is the format of the command:

```
show interface port access-group
```

The following example displays the ACLs assigned to ports 1 to 5:

```
awplus# show interface port1.0.1-port1.0.5 access-
group
```

```
Interface port1.0.1

    access-group 3010

    access-group 3002

Interface port1.0.2

    access-group 3025
```

Figure 198. SHOW INTERFACE ACCESS-GROUP Command

Displaying ACLs Assigned to VTY Lines

Use the SHOW RUNNING-CONFIG command to display the ACLs assigned to VTY lines. Here is the format of the command:

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

See Figure 199 for an example of the display that pertains to ACLs assigned to VTY lines. For more information about this command, see "SHOW RUNNING-CONFIG" on page 158.

```
!
line vty 0 9
    access-class 4000
    access-class 4001
!
```

Figure 199. SHOW RUNNING-CONFIG Command

Chapter 74
ACL Commands

The Access Control List (ACL) commands are summarized in Table 143 and described in detail within the chapter.

Table 143. Access Control List Commands

Command	Mode	Description
"ACCESS-CLASS" on page 1231	Virtual Terminal Line mode	Assigns an ACL to a VTY line.
"ACCESS-GROUP" on page 1233	Port Interface	Adds IP ACLs to ports.
"ACCESS-LIST (MAC Address)" on page 1235	Global Configuration	Creates ACLs that identify packets based on source and destination MAC addresses.
"ACCESS-LIST ICMP" on page 1238	Global Configuration	Creates ACLs that identify packets based on ICMP source and destination IP addresses.
"ACCESS-LIST IP" on page 1241	Global Configuration	Creates ACLs that filter packets based on source and destination IP addresses.
"ACCESS-LIST PROTO" on page 1245	Global Configuration	Creates ACLs that identify packets based on protocol numbers and source and destination IP addresses.
"ACCESS-LIST TCP" on page 1250	Global Configuration	Creates access control lists that filter ingress packets based on TCP port numbers.
"ACCESS-LIST UDP" on page 1254	Global Configuration	Creates access control lists that identify ingress packets based on UDP port numbers.
"MAC ACCESS-GROUP" on page 1258	Global Configuration	Adds MAC address ACLs to ports on the switch.
"NO ACCESS-LIST" on page 1259	Global Configuration	Deletes ACLs from the switch.
"NO ACCESS-GROUP" on page 1260	Port Interface	Removes ACLs from ports on the switch.

Table 143. Access Control List Commands (Continued)

Command	Mode	Description
"NO MAC ACCESS-GROUP" on page 1261	Port Interface	Removes MAC address ACLs from ports on the switch.
"SHOW ACCESS-LIST" on page 1262	Privileged Exec	Displays the ACLs on the switch.
"SHOW INTERFACE ACCESS-GROUP" on page 1264	Privileged Exec	Displays the port assignments of the ACLs.

ACCESS-CLASS

Syntax

access-class *<3000 – 3699>|<4000 – 4699>*

Parameters

3000 - 3699

Specifies the ID number of the access control list. The range is 3000 to 3699.

4000 - 4699

Specifies the ID number of the MAC access control list. The range is 4000 to 4699.

Mode

Virtual Terminal Line mode

Description

Use this command to assign an Access Control List to a VTY. This is done to restrict the remote access of the switch via Telnet, Web, SNMP, or SSH access. You can add one ACL to multiple VTY lines with this command.

> **Note**
> Allied Telesis recommends specifying all ten of the VTY lines with the ACCESS-LIST command because the switch assigns VTY lines randomly.

Use the no version of this command, NO ACCESS-CLASS, to remove an ACL assignment from the VTY lines.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example assigns the switch an IP address of 10.0.0.20/24. It creates a Numbered ACL with an ID of 3022 that allows IP address 10.0.0.3 full access to the switch. Then it creates an ACL with an ID number of 3025 that denies all IP addresses access to the switch.

It assigns ACL 3022 to VTY lines 0 through 9. Finally, ACL 3025 is assigned to VTY lines 0 through 9. The result is that IP address 10.0.0.3 has full remote access to the switch. All other IP addresses are denied remote access to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address 10.0.0.20/24
awplus(config-if)# quit
awplus(config)# access-list 3022 permit ip host 10.0.0.3
host 10.0.0.20
awplus(config)# access-list 3025 deny ip any host 10.0.0.20
awplus(config)# line vty 0 9
awplus(config-line)# access-class 3022
awplus(config-line)# access-class 3025
```

1232

ACCESS-GROUP

Syntax

access-group *id_number*

Parameters

id_number
> Specifies the ID number of an access control list you want to add to a port. The range is 3000 to 3699. You can add one ACL to a port at a time with this command.

Mode

Port Interface mode

Description

Use this command to add IP ACLs to ports on the switch. Ports begin to filter packets as soon as they are assigned ACLs. This command works for all ACLs, except for MAC address ACLs, which are added to ports with the MAC ACCESS-GROUP command. See "MAC ACCESS-GROUP" on page 1258.

Note
If a port is to have both permit and deny ACLs, you must add the permit ACLs first because ingress packets are compared against the ACLs in the order in which they are added to a port. If you add the deny ACLs before the permit ACLs, a port is likely to block traffic you want it to forward.

Use the no version of this command, NO ACCESS-GROUP, to remove IP ACL from a port on the switch.

Confirmation Command

"SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example adds an IP ACL with an ID of 3022 to port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# access-group 3022
```

This example removes an IP ACL with an ID of 3001 from port 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.7
awplus(config-if)# no access-group 3001
```

ACCESS-LIST (MAC Address)

Syntax

```
access-list id_number action src_mac_address|any
src_mac_mask dst_mac_address|any dst_mac_mask
```

Parameters

id_number

Specifies the ID number for the new ACL. The range is from 4000 to 4699.

action

Specifies the action of the ACL. Here are the possible actions:

permit: Forwards all ingress packets that match the ACL.

deny: Discards all ingress packets that match the ACL.

copy-to-mirror: Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

src_mac_address

Specifies the source MAC address of the ingress packets. Here are the possible options:

src_mac_address: Specifies the source MAC address of the packets. The address must be entered in hexadecimal in one of the following formats:

xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

any: Matches any source MAC address.

src_mac_mask

Specifies the source MAC address mask. The mask must be entered in one of the following formats:

xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

Assign the "x" variable a value of either "0" or "F." Specify "0" to indicate the parts of the MAC address the ACL is to filter. Specify "F" for parts of the MAC address the ACL should ignore.

Do not include a mask if you specified ANY as the source MAC address.

dst_mac_address

Specifies the destination MAC address of the ingress packets. Choose from the following options:

dst_mac_address: Specifies the destination MAC address of the packets. The address must be entered in hexadecimal in one of the following formats:

xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

any: Matches any destination MAC address.

dst_mac_mask

Specifies the destination MAC address mask. The mask must be entered in one of the following formats:

xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

Assign the "x" variable a value of either "0" or "F." Specify "0" to indicate the parts of the MAC address the ACL is to filter. Specify "F" for parts of the MAC address the ACL should ignore.

Mode

Global Configuration mode

Description

Use this command to create ACLs that filter packets based on source and destination MAC addresses.

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example configures port 3 to accept packets only from three specific devices:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 4001 permit 12:a3:4b:89:10:98
00:00:00:00:00:00 any
awplus(config)# access-list 4002 permit 00:8b:2a:56:11:80
00:00:00:00:00:00 any
awplus(config)# access-list 4003 permit 76:9a:8c:b2:88:1a
00:00:00:00:00:00 any
awplus(config)# access-list 4011 deny any any
awplus(config)# interface port1.0.3
awplus(config_if)# mac access-group 4001
```

1236

```
awplus(config_if)# mac access-group 4002
awplus(config_if)# mac access-group 4003
awplus(config_if)# mac access-group 4011
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.3 access-group
```

This example configures a 28-port switch to block Cisco Discovery Protocol (CDP) packets on all ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 4001 deny any 01:00:0c:cc:cc:cc
00:00:00:00:00:00
awplus(config)# interface port1.0.1-port1.0.28
awplus(config-if)# mac access-group 4001
awplus(config-if)# end
awplus# show access-list
awplus# show interface port1.0.1-port1.0.28 access-group
```

This example configures port 7 to accept only those packets that have source MAC addresses starting with 45:2A:B5:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 4025 permit 45:2a:b5:00:00:00
00:00:00:ff:ff:ff any
awplus(config)# access-list 4055 deny any any
awplus(config)# interface port1.0.7
awplus(config_if)# mac access-group 4025
awplus(config_if)# mac access-group 4055
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.7 access-group
```

This example configures port 19 to reject packets containing destination MAC addresses starting with A4:54:86:12:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 4102 deny any a4:54:86:12:00:00
00:00:00:00:ff:ff
awplus(config)# interface port1.0.19
awplus(config_if)# mac access-group 4102
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.19 access-group
```

ACCESS-LIST ICMP

Syntax

```
access-list id_number action icmp src_ipaddress
dst_ipaddress [vlan vid]
```

Parameters

id_number

Specifies an ID number for a new ACL. The range is 3000 to 3699. Each access list on the switch must have a unique ID number.

action

Specifies the action of the ACL. Here are the possible actions:

permit: Forwards all ingress packets that match the ACL.

deny: Discards all ingress packets that match the ACL.

copy-to-mirror: Copies all ingress packets that match the ACL to the destination port of the port mirror. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

scr_ipaddress

Specifies the source IP address of the ingress packets the access list should filter. Here are the possible options:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a source IP address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits of the network section of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24".

host ipaddress: Matches packets with a source IP address and is an alternative to the IPADRESS/MASK variable for addresses of specific end nodes. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

dst_ipaddress

Specifies the destination IP address of the ingress packets the access list should filter. Here are the possible options:

any: Matches any IP address.

1238

ipaddress/mask: Matches packets that have a destination IP address of a specific subnet or end node.

host ipaddress: Matches packets with a destination IP address of a specific end node. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

vlan

Indicates a VLAN identifier. Specify a VLAN if you want the ACL to filter tagged packets. Omit a VLAN if you want the ACL to filter untagged packets. Specify a value between 1 and 4094. You can enter only one VID.

Mode

Global Configuration mode

Description

Use this command to create Numbered IPv4 ACLs that identify traffic flows based on ICMP and source and destination IP addresses.

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example adds a deny access list to port 16 so that it discards all untagged ingress packets that are ICMP, regardless of their source or destination address. The access list is assigned the ID number 3012. Since the VID parameter is not included, this ACL applies to untagged packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3012 deny icmp any any
awplus(config)# interface port1.0.16
awplus(config_if)# access-group 3012
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.16 access-group
```

1239

This example adds a deny access list to ports 4 and 5 to discard all untagged ingress packets that are ICMP, from the 152.12.45.0 subnet. The access list is assigned the ID number 3094:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3094 deny icmp 152.12.45.0/24
any
awplus(config)# interface port1.0.4,port1.0.5
awplus(config_if)# access-group 3094
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.4,port1.0.5 access-group
```

This example adds a deny access list to port 11 to discard all ingress packets that are ICMP and that have source and destination addresses from the 115.201.312.0/24 and 115.201.313.0/24 subnets, respectively. The ACLs are assigned the ID numbers 3045 and 3046:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3045 deny icmp 115.201.312.0/24
115.201.313.0/24
awplus(config)# access-list 3046 deny icmp 115.201.312.0/24
115.201.313.0/24
awplus(config)# interface port1.0.11
awplus(config_if)# access-group 3045
awplus(config_if)# access-group 3046
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.11 access-group
```

This example creates a deny access list that discards all tagged ingress IGMP packets with a VID of 12, from ports 12 to 20:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3156 deny icmp any any vlan 12
awplus(config)# interface port1.0.12-port1.0.20
awplus(config_if)# access-group 3156
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.12-port1.0.20 access-group
```

ACCESS-LIST IP

Syntax

```
access-list id_number action ip src_ipaddress dst_ipaddress
[vlan vid]
```

Parameters

id_number

> Specifies the ID number for a new ACL. The range is 3000 to 3699.

action

> Specifies the action of the access list. Here are the possible actions:

> > *permit:* Forwards all ingress packets that match the ACL.

> > *deny:* Discards all ingress packets that match the ACL.

> > *copy-to-mirror:* Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

scr_ipaddress

> Specifies the source IP address of the ingress packets the access list should filter. Here are the possible options:

> > *any:* Matches any IP address.

> > *ipaddress/mask*: Matches packets that have a source IP address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits of the network section of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24".

> > *host ipaddress*: Matches packets with a source IP address and is an alternative to the IPADRESS/MASK variable for addresses of specific end nodes. The HOST keyword indicates that the address is of a specific and node and that no mask is required.

dst_ipaddress: Specifies the destination IP address of the ingress packets the access list should filter. Here are the possible options:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a destination IP address of a specific subnet or end node.

host ipaddress: Matches packets with a destination IP address of a specific end node. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

vlan

Indicates a VLAN identifier. Specify a VLAN if you want the ACL to filter tagged packets. Omit a VLAN if you want the ACL to filter untagged packets. Specify a value between 1 and 4094. You can enter only one VID.

Mode

Global Configuration mode

Description

Use this command to create ACLs that identify traffic flows based on the source and destination IP addresses of the packets.

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example adds a deny ACL, ID number 3201, that discards all untagged ingress packets from the 149.11.124.0 subnet, on ports 4 and 9:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3201 deny ip 149.11.124.0/24 any
awplus(config)# interface port1.0.4,port1.0.9
awplus(config_if)# access-group 3201
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.4,port1.0.9 access-group
```

This example creates a deny access list, ID number 3095, that discards all untagged ingress packets that have destination addresses in the 149.112.2.0 subnet, on ports 11 to 13:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3095 deny ip any 149.112.2.0/24
awplus(config)# interface port1.0.11-port1.0.13
awplus(config_if)# access-group 3095
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.11-port1.0.13 access-group
```

This example creates a deny access list, ID number 3202, that discards all tagged ingress packets on port 24 that are from the 157.11.21.0 subnet and are going to an end node with the IP address 157.11.21.45. The VID of the tagged packets is 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3202 deny ip 157.11.21.0/24
157.11.21.45/32 vlan 15
awplus(config)# interface port1.0.24
awplus(config_if)# access-group 3202
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.24 access-group
```

This example is the same as the previous example, except the HOST keyword is used to indicate the IP address of the destination node:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3202 deny ip 157.11.21.0/24 host
157.11.21.45 vlan 15
awplus(config)# interface port1.0.24
awplus(config_if)# access-group 3202
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.24 access-group
```

This example configures ports 22 and 23 to accept only untagged ingress packets containing destination addresses in the 149.124.47.0 subnet. This example requires both permit and deny ACLs because the permitted traffic is a subset of all traffic on the ports. The permit ACL, ID number 3011, specifies the 149.124.47.0 subnet and the deny ACL, ID number 3012, defines all traffic. The permit access list is added first to the ports with the ACCESS-GROUP command so that packets are compared against it first, before the deny ACL:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3011 permit ip any 149.124.47.0/
24
awplus(config)# access-list 3012 deny ip any any
awplus(config)# interface port1.0.22,port1.0.23
awplus(config_if)# access-group 3011
awplus(config_if)# access-group 3012
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.22,port1.0.23 access-group
```

This example configures ports 17 and 18 to accept untagged ingress packets from the 149.82.134.0 subnet, and to discard all other packets. As in the previous example, both a permit access list and a deny access list are required. The allowed traffic is defined with a permit ACL, which is given the ID number 3022. The deny ACL, with the ID number 3101, specifies all traffic:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3022 permit ip any 149.82.134.0/
24 vlan 22
awplus(config)# access-list 3010 deny ip any any
awplus(config)# interface port1.0.17,port1.0.18
awplus(config_if)# access-group 3022
awplus(config_if)# access-group 3101
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.17,port1.0.18 access-group
```

ACCESS-LIST PROTO

Syntax

```
access-list id_number action proto protocol_number
src_ipaddress dst_ipaddress [vlan vid]
```

Parameters

id_number

Specifies an ID number for a new ACL. The range is 3000 to 3699. Each access list on the switch must have a unique ID number.

action

Specifies the action of the ACL. Choose from the possible actions:

permit: Forwards all ingress packets that match the ACL.

deny: Discards all ingress packets that match the ACL.

copy-to-mirror: Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

protocol_number

Specifies a protocol number. You can specify one protocol number. Refer to Table 144, "Protocol Numbers" on page 1246 for the list of protocol numbers.

scr_ipaddress

Specifies the source IP address of the ingress packets the access list should filter. Choose one of the following:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a source IP address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits of the network section of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24".

host ipaddress: Matches packets with a source IP address and is an alternative to the IPADRESS/MASK variable for addresses of specific end nodes. The HOST keyword indicates that the address is of a specific and node and that no mask is required.

dst_ipaddress

Specifies the destination IP address of the ingress packets the access list should filter. Choose one of the following:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a destination IP address of a specific subnet or end node.

host ipaddress: Matches packets with a destination IP address of a specific end node. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

vlan

Indicates a VLAN identifier. Specify a VLAN if you want the ACL to filter tagged packets. Omit a VLAN if you want the ACL to filter untagged packets. Specify a value between 1 and 4094. You can enter only one VID.

Mode

Global Configuration mode

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Description

Use this command to create ACLs that identify traffic flows based on protocol numbers and source and destination IP addresses. The protocol numbers are listed in Table 144.

Table 144. Protocol Numbers

Number	Description
1	Internet Control Message (RFC792)
2	Internet Group Management (RFC1112)
3	Gateway-to-Gateway (RFC823)
4	IP in IP (RFC2003)
5	Stream (RFC1190 and RFC1819))
6	TCP (Transmission Control Protocol) (RFC793)
8	EGP (Exterior Gateway Protocol) (RFC888)

Table 144. Protocol Numbers (Continued)

Number	Description
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]
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

Table 144. Protocol Numbers (Continued)

Number	Description
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 - 254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example adds a deny access list to port 2 to discard all untagged ingress packets of protocol 28, regardless of the source or destination address. The access list is assigned the ID number 3016:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3016 deny proto 28 any any
awplus(config)# interface port1.0.2
awplus(config_if)# access-group 3016
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.2 access-group
```

This example adds a deny access list to ports 5 and 6 so that they discard all tagged ingress packets that have the protocol 17 number and the VID 12, and are from the 152.12.45.0 subnet. The access list is assigned the ID number 3011:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3011 deny proto 17 152.12.45.0/
24 any vlan 12
awplus(config)# interface port1.0.5,port1.0.6
```

```
awplus(config_if)# access-group 3011
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.5,port1.0.6 access-group
```

This example configures port 18 to accept untagged packets only from the 167.75.89.0 network and that are protocol 54. The permit ACL is assigned the ID number 3014 and the deny ACL, which blocks all protocol 54 packets, is assigned the ID number 3025:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3014 permit proto 54
167.75.89.0/24 any
awplus(config)# access-list 3025 deny proto 54 any any
awplus(config)# interface port1.0.18
awplus(config_if)# access-group 3014
awplus(config_if)# access-group 3025
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.18 access-group
```

ACCESS-LIST TCP

Syntax

```
access-list id_number action tcp src_ipaddress
eq|lt|gt|ne|range src_tcp_port dst_ipaddress
eq|lt|gt|ne|range dst_tcp_port [vlan vid]
```

Parameters

id_number

Specifies an ID number for a new ACL. The range is 3000 to 3699.

action

Specifies the action of the ACL. Choose one of the following:

permit: Forwards all ingress packets that match the ACL.

deny: Discards all ingress packets that match the ACL.

copy-to-mirror: Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

src_ipaddress

Specifies the source IP address of the ingress packets the access list should filter. Choose one of the following:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a source IP address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits of the network section of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24".

host ipaddress

Matches packets with a source IP address and is an alternative to the IPADRESS/MASK variable for addresses of specific end nodes. The HOST keyword indicates that the address is of a specific and node and that no mask is required.

eq

Matches packets that are equal to the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

1250

lt

Matches packets that are less than the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

gt

Matches packets that are greater than the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

ne

Matches packets that are not equal to the TCP port number specified by the SRC_TCP_PORT or DST_TCP_PORT parameter.

range

Matches packets with TCP port numbers within the range. Separate the numbers of the range by a space, for instance:

range 4 10

src_tcp_port

Specifies the source TCP port number. The range is 0 to 65535. Omit this parameter if you are entering a range of TCP port numbers.

dst_ipaddress

Specifies the destination IP address of the ingress packets the access list should filter. Here are the possible options:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a destination IP address of a specific subnet or end node.

host ipaddress: Matches packets with a destination IP address of a specific end node. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

dst_tcp_port

Specifies the destination TCP port number. The range is 0 to 65535. Omit this parameter if you are entering a range of port numbers.

vlan

Indicates a VLAN identifier. Specify a VLAN if you want the ACL to filter tagged packets. Omit a VLAN if you want the ACL to filter untagged packets. Specify a value between 1 and 4094. You can enter only one VID.

Mode

Global Configuration mode

Description

Use this command to create access control lists that filter ingress packets based on TCP port numbers.

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example creates an ACL, ID number 3045, that discards all untagged ingress TCP packets on port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3045 deny tcp any range 0 65535
any range 0 65535
awplus(config)# interface port1.0.5
awplus(config_if)# access-group 3045
```

This example creates an ACL that discards all untagged ingress packets that have the source and destination TCP port number 165. The ACL is applied to port 1 and assigned the ID number 3078:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3078 deny tcp any eq 165 any eq
165
awplus(config)# interface port1.0.1
awplus(config_if)# access-group 3078
```

This example defines an ACL that causes port 18 to discard all untagged ingress TCP packets that have source and destination TCP port numbers in the range of 12 to 100 and that are going to the 149.123.159.0 subnet. The list is assigned the ID number 3126:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3126 deny tcp any range 12 100
149.123.159.0/24 range 12 100
awplus(config)# interface port1.0.18
awplus(config_if)# access-group 3126
```

This example creates an ACL that causes port 14 to discard all tagged ingress TCP packets with the VID 27, regardless of their source or destination TCP port numbers. The list is assigned the ID number 3255:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3255 deny tcp any any vlan 27
awplus(config)# interface port1.0.14
awplus(config_if)# access-group 3255
```

This example configures port 21 to forward untagged TCP port 67 to 87 packets only if they are from the 154.11.234.0 network and are going to the 154.11.235.0 network. This example requires a permit ACL because the permitted traffic, TCP packets with port numbers in the range of 67 to 87, is a subset of all TCP packets on the port:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3017 permit tcp 154.11.234.0/24
range 67 87 154.11.235.0/24 range 67 87
awplus(config)# access-list 3005 deny tcp any any range 67
87
awplus(config)# interface port1.0.21
awplus(config_if)# access-group 3017
awplus(config_if)# access-group 3005
```

ACCESS-LIST UDP

Syntax

```
access-list id_number action udp src_ipaddress
eq|lt|gt|ne|range src_udp_port dst_ipaddress
eq|lt|gt|ne|range dst_udp_port vlan vid
```

Parameters

id_number

Specifies an ID number for a new ACL. The range is 3000 to 3699.

action

Specifies the action of the ACL. Choose one of the following:

permit: Forwards all ingress packets that match the ACL.

deny: Discards all ingress packets that match the ACL.

copy-to-mirror: Copies all ingress packets that match the ACL to the destination port of the mirror port. This action must be used in conjunction with the port mirror feature, explained in Chapter 21, "Port Mirror" on page 407.

src_ipaddress

Specifies the source IP address of the ingress packets the access list should filter. Here are the possible options:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a source IP address of a subnet or an end node. The mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits of the network section of the address. The IP address and the mask are separated by a slash (/); for example, "149.11.11.0/24".

host ipaddress: Matches packets with a source IP address and is an alternative to the IPADRESS/MASK variable for addresses of specific end nodes. The HOST keyword indicates that the address is of a specific and node and that no mask is required.

eq

Matches packets that are equal to the UDP port number specified by the SRC_UDP_PORT or DST_UDP_PORT parameter.

lt

Matches packets that are less than the UDP port number specified by the SRC_UDP_PORT or DST_UDP_PORT parameter.

gt

Matches packets that are greater than the UDP port number specified by the SRC_UDP_PORT or DST_UDP_PORT parameter.

ne

Matches packets that are not equal to the UDP port number specified by the SRC_UDP_PORT or DST_UDP_PORT parameter.

range

Matches packets with UDP port numbers within the range. Separate the numbers of the range by a space. For instance:

range 4 10

src_udp_port

Specifies the source UDP port number. The range is 0 to 65535. Omit this parameter if you are entering a range of UDP port numbers.

dst_ipaddress

Specifies the destination IP address of the ingress packets the access list should filter. Here are the possible options:

any: Matches any IP address.

ipaddress/mask: Matches packets that have a destination IP address of a specific subnet or end node.

host ipaddress: Matches packets with a destination IP address of a specific end node. The HOST keyword indicates that the address is of a specific end node and that no mask is required.

dst_udp_port

Specifies the destination UDP port number. The range is 0 to 65535. Omit this parameter if you are entering a range of port numbers.

vlan

Indicates a VLAN identifier. Specify a VLAN if you want the ACL to filter tagged packets. Omit a VLAN if you want the ACL to filter untagged packets. Specify a value between 1 and 4094. You can enter only one VID.

1255

Mode

Global Configuration mode

Description

Use this command to create access control lists that filter ingress packets based on UDP port numbers.

Confirmation Commands

"SHOW ACCESS-LIST" on page 1262 and "SHOW INTERFACE ACCESS-GROUP" on page 1264

Examples

This example creates a Numbered IPv4 ACL, with an ID number of 3118, that discards all untagged ingress UDP packets on ports 18 and 19:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3118 deny udp any range 0 65535
any range 0 65535
awplus(config)# interface port1.0.18,port1.0.19
awplus(config_if)# access-group 3118
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.18,port1.0.19 access-group
```

This example creates an ACL that discards all tagged ingress packets that have the source and destination UDP port number 10 and the VID 29. The ACL is applied to port 17 and assigned the ID number 3091:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3091 deny udp any eq 10 any eq
10 vlan 29
awplus(config)# interface port1.0.17
awplus(config_if)# access-group 3091
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.17 access-group
```

This example defines an ACL that causes port 18 to discard all untagged ingress packets that have source and destination UDP port numbers in the range of 12 to 100 and that are going to the 149.123.159.0 subnet. The VLAN parameter is also included to restrict the ACL to UDP packets that belong to VLAN 7. The list is assigned the ID number 3078:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3078 deny udp any range 12 100
149.123.159.0/24 range 12 100 vlan 7
awplus(config)# interface port1.0.18
awplus(config_if)# access-group 3078
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.18 access-group
```

This example configures port 21 to forward tagged UDP port 67 to 87 packets only if they are from the 154.11.234.0 network and are going to the 154.11.235.0 network, and have the VID 20. This example requires a permit ACL because the permitted traffic, UDP packets with port numbers in the range of 67 to 87, is a subset of all UDP packets on the port:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 3119 permit udp 154.11.234.0/24
range 67 87 154.11.235.0/24 range 67 87 vlan 20
awplus(config)# access-list 3005 deny udp any any range 67
87
awplus(config)# interface port1.0.21
awplus(config_if)# access-group 3119
awplus(config_if)# access-group 3005
awplus(config_if)# end
awplus# show access-list
awplus# show interface port1.0.21 access-group
```

MAC ACCESS-GROUP

Syntax

```
mac access-group id_number
```

Parameters

id_number

Specifies the ID number of a MAC address access control list you want to add to a port. The range is 4000 to 4699.

Mode

Port Interface mode

Description

Use this command to add MAC address ACLs to ports on the switch. Ports begin to filter packets as soon as they are assigned ACLs. You can add one ACL to a port at a time with this command.

Use the no version of this command, NO MAC ACCESS-LIST, to remove a MAC address ACL from a switch.

Note

If a port is to have both permit and deny ACLs, you must add the permit ACLs first because ingress packets are compared against the ACLs in the order in which they are added to a port. If you add the deny ACLs before the permit ACLs, a port is likely to block traffic you want it to forward.

Confirmation Command

"SHOW INTERFACE ACCESS-GROUP" on page 1264

Example

This example adds the ACL 4022 to port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# mac access-group 4022
awplus(config-if)# end
awplus# show interface port1.0.15 access-group
```

NO ACCESS-LIST

Syntax

```
no access-list id_number
```

Parameters

id_number
Specifies the ID number of an access list you want to delete from the switch. You can delete one access list at a time with this command.

Mode

Global Configuration mode

Description

Use this command to delete ACLs from the switch. ACLs must first be removed from their port assignments before they can be deleted. For instructions, refer to "NO ACCESS-GROUP" on page 1260 and "NO MAC ACCESS-GROUP" on page 1261.

Confirmation Command

"SHOW ACCESS-LIST" on page 1262

Example

This example deletes the access list with the ID number 3015 from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no access-list 3015
awplus(config-if)# end
awplus# show access-list
```

NO ACCESS-GROUP

Syntax

```
no access-group id_number
```

Parameters

id_number
> Specifies the ID number of an access list. The range is 3000 to 3699. You can remove one ACL from a port at a time with this command.

Mode

Port Interface mode

Description

Use this command to remove ACLs from ports on the switch. This command works for all ACLs, except for MAC address ACLs, which are removed with "NO MAC ACCESS-GROUP" on page 1261.

Confirmation Command

"SHOW INTERFACE ACCESS-GROUP" on page 1264

Example

This example removes the ACL with the ID number 3121 from port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no access-group 3121
awplus(config-if)# end
awplus# show interface port1.0.23 access-group
```

NO MAC ACCESS-GROUP

Syntax

```
no mac access-group id_number
```

Parameters

id_number
> Specifies the ID number of a MAC address access list to be removed from a port. The range is 4000 to 4699 You can remove one ACL from a port at a time with this command.

Mode

Port Interface mode

Description

Use this command to remove MAC address ACLs from ports on the switch.

Confirmation Command

"SHOW INTERFACE ACCESS-GROUP" on page 1264

Example

This example removes a MAC address ACL with the ID number 4014 from port 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# no mac access-group 4014
awplus(config-if)# end
awplus# show interface port1.0.16 access-group
```

SHOW ACCESS-LIST

Syntax

show access-list [*<3000-3699>*|*<4000-4699>*|*<list-name>*]

Parameters

<3000-3699>
Indicates a Numbered IP ACL.

<4000-4699>
Indicates a MAC ACL.

list-name
Indicates a Named IP ACL.

Mode

Privileged Exec mode

Description

Use this command to display the configurations of the Numbered IPv4, MAC, and Named IPv4 ACLs on the switch. If you do not specify an option, all three ACL types are displayed.

To display the port assignments of the ACLs, refer to "SHOW INTERFACE ACCESS-GROUP" on page 1264.

Example

This example displays Numbered IP, MAC, and Named IP ACLs:

awplus# show access-list

```
IP access-list 3104
    deny 149.87.201.1 mask 255.255.255.0 any
MAC access-list 4400
    permit any any
IP access-list icmppermit
    ICMP permit an any time-range daily
IP access-list denytcp
    TCP deny 149.55.65.0 mask 255.255.255.0 any time-range NONE

Total number of access-lists= 4
```

Figure 200. SHOW ACCESS-LIST Command

SHOW INTERFACE ACCESS-GROUP

Syntax

```
show interface port access-group
```

Parameters

port
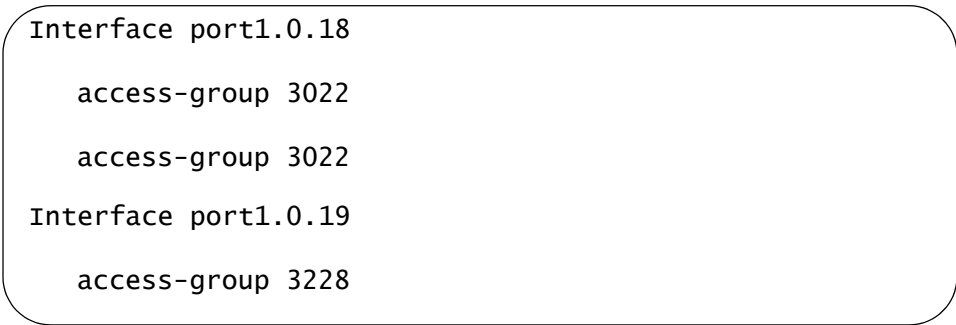
Specifies a port number. You can specify more than one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display the port assignments of the ACLs. Here is an example of the information.

```
Interface port1.0.18

    access-group 3022

    access-group 3022

 Interface port1.0.19

    access-group 3228
```

Figure 201. SHOW INTERFACE ACCESS-GROUP Command

Example

This example displays the ID numbers of the ACLs assigned to ports 1 and 2:

```
awplus# show interface port1.0.1,port1.0.2 access-group
```

Chapter 75

Quality of Service (QOS) Commands

The Quality of Service (QoS) commands are summarized in Table 145.

Table 145. Quality of Service Commands

Command	Mode	Description
"MLS QOS ENABLE" on page 1267	Global Configuration	Activates QoS on the switch.
"MLS QOS MAP COS-QUEUE" on page 1268	Port Interface	Maps CoS priorities to port egress queues.
"MLS QOS MAP DSCP-QUEUE" on page 1270	Port Interface	Maps DSCP priorities to port egress queues.
"MLS QOS QUEUE" on page 1272	Port Interface	Configures the default egress queue for any packet arriving on the port.
"MLS QOS SET COS" on page 1273	Port Interface	Remarks all egress packets on a port with the specified CoS value.
"MLS QOS SET DSCP" on page 1274	Port Interface	Remarks all egress packets on a port with the specified DSCP value.
"MLS QOS TRUST COS" on page 1275	Port Interface	Configures ports to use the CoS priorities in ingress packets to determine the queues on the egress ports.
"MLS QOS TRUST DSCP" on page 1276	Port Interface	Configures ports to use the DSCP priorities in ingress packets to determine the appropriate queues on the egress ports to store the packets.
"NO MLS QOS ENABLE" on page 1277	Global Configuration	Disables QoS on the switch.
"NO WRR-QUEUE WEIGHT" on page 1278	Port Interface	Set the CoS scheduling method on the ports to strict priority.
"SHOW MLS QOS INTERFACE" on page 1279	Privileged Exec	Display the scheduling methods of the ports and, for weighted round robin scheduling, the assignments of weights to egress queues.

Table 145. Quality of Service Commands

Command	Mode	Description
"SHOW MLS QOS MAPS COS-QUEUE" on page 1282	Privileged Exec	Displays the mappings of CoS priority values to egress queues.
"SHOW MLS QOS MAPS DSCP-QUEUE" on page 1283	Privileged Exec	Displays the mappings of DSCP priority values to port egress queues.
"WRR-QUEUE WEIGHT" on page 1285	Port Interface	Sets the QoS scheduling method to weighted round robin.

MLS QOS ENABLE

Syntax

```
mls qos enable
```

Parameters

None.

Mode

Global Configuration mode

Description

Use this command to activate QoS on the switch so that ingress packets are stored in egress queues according to their CoS or DSCP values.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# mls qos enable
```

MLS QOS MAP COS-QUEUE

Syntax

```
mls qos map cos-queue cos_priority to egress_queue
```

Parameters

cos_priority   Specifies a Class of Service (CoS) priority level of 0, lowest priority, through 7, highest priority. An egress queue can have more than one priority level, but you can specify just one priority level at a time with this command.

egress_queue Specifies an egress queue number of 0 through 7, The lowest priority queue is 0 and the highest queue is 7. You can specify just one queue.

Mode

Port Interface mode

Description

Use this command to map CoS priorities to port egress queues. An egress queue can have more than one priority, but you can assign just one priority at a time with this command.

> **Note**
> QoS must be enabled on the switch and a port must be set to CoS trust before you can use this command. Refer to commands "MLS QOS ENABLE" on page 1267 and "MLS QOS TRUST COS" on page 1275.

Use the NO form of this command to return the CoS priority mappings on ports to their default values.

Confirmation Command

"SHOW MLS QOS MAPS COS-QUEUE" on page 1282

Examples

This example maps priorities 1 and 2 to queue 5 and priority 3 to queue 6 on port 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18
```

```
awplus(config-if)# mls qos trust cos
awplus(config-if)# mls qos map cos-queue 1 to 5
awplus(config-if)# mls qos map cos-queue 2 to 5
awplus(config-if)# mls qos map cos-queue 3 to 6
```

This example restores the default mappings of the CoS priorities to the egress queues on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no mls qos map cos-queue
```

MLS QOS MAP DSCP-QUEUE

Syntax

```
mls qos map dscp-queue dscp_priority to egress_queue
```

Parameters

dscp_priority   Specifies a DSCP priority level. The lowest priority is 0 and the highest priority is 63. You can map more than one priority level to an egress queue, but you can specify just one priority level at a time with this command.

egress_queue Specifies an egress queue number of 0 through 7, The lowest priority queue is 0 and the highest queue is 7. You can specify just one queue.

Mode

Port Interface mode

Description

Use this command to map DSCP priorities to port egress queues. An egress queue can have more than one priority, but you can assign just one priority at a time with this command.

Note
QoS must be enabled on the switch and a port must be set to DSCP trust before you can use this command. Refer to commands "MLS QOS ENABLE" on page 1267 and "MLS QOS TRUST DSCP" on page 1276.

Use the NO form of this command to return the DSCP priority mappings on ports to their default values.

Confirmation Command

"SHOW MLS QOS MAPS DSCP-QUEUE" on page 1283

Examples

This example maps DSCP priorities 11 to 13 to queue 7 on port 14:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.14
awplus(config-if)# mls qos trust dscp
```

```
awplus(config-if)# mls qos map dscp-queue 11 to 7
awplus(config-if)# mls qos map cos-queue 12 to 7
awplus(config-if)# mls qos map cos-queue 13 to 7
```

This example restores the default mappings of the DSCP priorities to the egress queues on port 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no mls qos map dscp-queue
```

MLS QOS QUEUE

Syntax

```
mls qos queue priority
```

Parameters

priority   Specifies a Class of Service (CoS) priority level of 0, lowest priority, to 7, highest priority. You can specify just one priority level.

Mode

Port Interface mode

Description

Use this command to configure the default egress queue for any packet arriving on the port. When no default queue is configured the cos-queue map is used to choose the queue for packets.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example assigns queue 7 as the default queue for port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# mls qos queue 7
```

This example removes the default queue from port 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16
awplus(config-if)# no mls qos queue
```


MLS QOS SET COS

Syntax

```
mls qos set cos priority
```

Parameters

priority   Specifies a Class of Service (CoS) priority level of 0, lowest
                priority, to 7, highest priority. You can specify just one
                priority level.

Mode

Port Interface mode

Description

Use this command to remark all egress packets on a port with the
specified CoS value.

Use the NO form of this command to remove remark CoS values from
ports.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example configures port 12 to add or change the CoS priority in all
egress packets to 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# mls qos set cos 5
```

This example removes the remark CoS value from port 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no mls qos set cos
```

MLS QOS SET DSCP

Syntax

```
mls qos set dscp priority
```

Parameters

priority   Specifies a DSCP priority level of 0, lowest priority, to 63, highest priority. You can specify just one priority level.

None.

Mode

Port Interface mode

Description

Use this command to remark all egress packets on a port with the specified DSCP value.

Use the NO form of this command to remove remark DSCP values from ports.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example configures port 3 to add or change the DSCP value in all egress packets to 27:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mls qos set dscp 27
```

This example removes the remark DSCP value from port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# no mls qos set dscp
```

MLS QOS TRUST COS

Syntax

```
mls qos trust cos
```

Parameters

None.

Mode

Port Interface mode

Description

Use this command to configure ports to use the CoS priorities in ingress packets to determine the appropriate queues on the egress ports to store the packets.

> **Note**
> QoS must be enabled on the switch before you can use this command.

Use the NO form of this command to stop ports from using the CoS priorities in ingress packets to determine the egress queues.

Confirmation Command

"SHOW MLS QOS INTERFACE" on page 1279

Example

This example configures ports 1 and 2 to use the CoS values of the ingress packets when directing packets to the queues on the egress ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# mls qos trust cos
```

MLS QOS TRUST DSCP

Syntax

```
mls qos trust dscp
```

Parameters

None.

Mode

Port Interface mode

Description

Use this command to configure ports to use the DSCP priorities in ingress packets to determine the appropriate queues on the egress ports to store the packets.

Note
QoS must be enabled on the switch before you can use this command.

Use the NO form of this command to stop ports from using the DSCP priorities in ingress packets to determine the egress queues.

Confirmation Command

"SHOW MLS QOS INTERFACE" on page 1279

Example

This example configures port 23 to use the DSCP values of the ingress packets when directing packets to queues on the egress ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.23
awplus(config-if)# mls qos trust dscp
```

NO MLS QOS ENABLE

Syntax

```
no mls qos enable
```

Parameters

None.

Mode

Global Configuration mode

Description

Use this command to disable QoS on the switch. When QoS is disabled, all traffic is treated the same.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no mls qos enable
```

NO WRR-QUEUE WEIGHT

Syntax

```
no wrr-queue weight
```

Parameters

None.

Mode

Port Interface mode

Description

Use this command to set the CoS scheduling method on the ports to strict priority so that they transmit packets from higher priority queues before packets in lower priority queues.

Confirmation Command

"SHOW MLS QOS INTERFACE" on page 1279

Example

This example configures ports 6 to 8 for the strict priority scheduling method:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.6-port1.0.8
awplus(config-if)# no wrr-queue weight
```

SHOW MLS QOS INTERFACE

Syntax

show mls qos interface *port*

Parameters

port　　　　　Specifies the port to display. You can view only one port at
　　　　　　　a time.

Mode

Privileged Exec mode

Description

Use this command to display the scheduling methods of the ports and, for
weighted round robin scheduling, the assignments of weights to egress
queues. Figure 202 and Figure 203 on page 1280 are examples of a port
set to strict priority.

```
Default CoS:    0
Default Queue: 2
Number of egress queues: 8
Trust:
Mark/Remark:
Egress Queue:       0
    Scheduler:      Strict Priority
    Weight:         N/A
Egress Queue:       1
    Scheduler:      Strict Priority
    Weight:         N/A
Egress Queue:       2
    Scheduler:      Strict Priority
    Weight:         N/A
Egress Queue:       3
    Scheduler:      Strict Priority
    Weight:         N/A
Egress Queue:       4
    Scheduler:      Strict Priority
    Weight:         N/A
Egress Queue:       5
    Scheduler:      Strict Priority
    Weight:         N/A
```

Figure 202. SHOW MLS QOS INTERFACE Command - Strict Priority

```
Egress Queue:         6
   Scheduler:         Strict Priority
   Weight:            N/A
Egress Queue:         7
   Scheduler:         Strict Priority
   Weight:            N/A
```

Figure 203. SHOW MLS QOS INTERFACE Command - Strict Priority (continued)

Figure 204 is an example of a port set to weighted round robin scheduling.

```
Default CoS:   0
Default Queue: 2
Number of egress queues: 8
Trust:
Mark/Remark:
Egress Queue:         0
   Scheduler:         Weighted Round Robin
   Weight:            1
Egress Queue:         1
   Scheduler:         Weighted Round Robin
   Weight:            1
Egress Queue:         2
   Scheduler:         Weighted Round Robin
   Weight:            5
Egress Queue:         3
   Scheduler:         Weighted Round Robin
   Weight:            5
Egress Queue:         4
   Scheduler:         Weighted Round Robin
   Weight:            10
Egress Queue:         5
   Scheduler:         Weighted Round Robin
   Weight:            10
Egress Queue:         6
   Scheduler:         Weighted Round Robin
   Weight:            15
Egress Queue:         7
   Scheduler:         Weighted Round Robin
   Weight:            15
```

Figure 204. SHOW MLS QOS INTERFACE Command - Weighted Round Robin

The fields in the display are described in Table 146.

Table 146. SHOW MLS QOS INTERFACE Command

Field	Description
Default CoS	Specifies the default CoS value for packets that do not have a value.
Default Queue	Specifies the default egress queue for packets that do not have a COS value.
Number of egress queues	Specifies the number of egress queues on the port. Each port on the switch has eight queues.
Trust	DSCP/CoS or empty
Egress Queue	Specifies the egress queue number.
Scheduler	Specifies the packet scheduling method. The possible settings are Strict Priority and Weighted Round Robin.
Weight	Specifies the weight of the queue, in number of packets. This applies only to weighted round robin. This is "N/A" for strict priority.

Example

This example displays the mappings of egress queues to CoS values for port 3:

```
awplus# show mls qos cos-queue port1.0.3
```

SHOW MLS QOS MAPS COS-QUEUE

Syntax

```
show mls qos maps cos-queue interface port
```

Parameters

port   Specifies the port to display. You can view only one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display the mappings of CoS priority values to port egress queues. An example of the information is shown in Figure 205.

```
Interface port1.0.1:
 COS-TO-QUEUE-MAP:
    COS :    0 1 2 3 4 5 6 7
   ---------------------------
    QUEUE :  2 0 1 3 4 5 6 7
```

Figure 205. SHOW MLS QOS MAPS COS-QUEUE Command

The CoS values in the first line are matched with the egress queue assignments in the second line. For example, in Figure 205 of port 1, packets with CoS 0 are placed in egress queue 2, packets with CoS 1 are placed in egress queue 0, and so on.

The mappings of CoS priorities and egress queues are set with "MLS QOS MAP COS-QUEUE" on page 1268.

Example

This example display the mappings of CoS priority values to port egress queues for port 17

```
awplus# show mls qos maps cos-queue interface port1.0.17
```

SHOW MLS QOS MAPS DSCP-QUEUE

Syntax

```
show mls qos maps dscp-queue interface port
```

Parameters

port   Specifies the port to display. You can view only one port at a time.

Mode

Privileged Exec mode

Description

Use this command to display the mappings of DSCP priority values to port egress queues. An example of the information is shown in Figure 206 on page 1284.

```
Interface port1.0.21
DSCP-TO-QUEUE-MAP:

--------------------
Queue: 0
DSCP: 0-7
--------------------
--------------------
Queue: 1
DSCP: 8-15
--------------------
--------------------
Queue: 2
DSCP: 16-23
--------------------
--------------------
Queue: 3
DSCP: 24-31
--------------------
--------------------
Queue: 4
DSCP: 32-39
--------------------
--------------------
Queue: 5
DSCP: 40-47
--------------------
--------------------
Queue: 6
DSCP: 48-55
--------------------
--------------------
Queue: 7
DSCP: 56-63
--------------------
```

Figure 206. SHOW MLS QOS MAPS DSCP-QUEUE Command

The mappings of DSCP priorities and egress queues are set with "MLS QOS MAP DSCP-QUEUE" on page 1270.

Example

This example displays the DSCP mappings for port 21:

awplus# show mls qos maps dscp-queue interface port1.0.21

WRR-QUEUE WEIGHT

Syntax

```
wrr-queue weight weights
```

Parameters

weights   Specifies the weights of a port's eight egress priority queues for the weighted round robin scheduling method. The ranges are 1 to 15 packets for Q0 to Q6 and 0 to 15 packets for Q7. A setting of 0 for Q7 means that its packets always take priority and that it has to be empty before a port transmits packets from the other queues.

The weights are specified in the following order:

Q0,Q1,Q2,Q3,Q4,Q5,Q6,Q7

You must specify all eight queues. For example, to assign a weight of 1 to Q0 and Q1, a weight of 5 to Q2 and Q3, a weight of 10 to Q4 and Q5, and a weight of 15 to Q6 and Q7, you enter this parameter as:

```
1,1,5,5,10,10,15,15
```

The default setting for all the queues is 1, giving all the queues have the same weight.

Mode

Port Interface mode

Description

Use this command to set the CoS scheduling method on the ports to weighted round robin and to assign weights to egress queues.

Confirmation Command

"SHOW MLS QOS INTERFACE" on page 1279

Example

This example configures port 3 to weighted round robin. It assigns a weight of 1 to egress priority queues Q0 and Q1, a weight of 10 to queues Q2 and Q3, and a weight of 15 to queues Q4 to Q7:

```
awplus> enable
awplus# configure terminal
```

```
awplus(config)# interface port1.0.3
awplus(config-if)# wrr-queue weight 1,1,10,10,15,15,15,15
```

Section XI
Management Security

This section contains the following chapters:

1288

Chapter 76

Local Manager Accounts

This chapter provides the following topics:

Overview

Each AT-9000 Series switch is pre-configured at the factory with one default manager account. The factory-default values for the user name and password are "manager" and "friend." If you are the only administrator of the switch, you may not need more than one manager account. But if you plan for the switch to be managed by more than one administrator, you may want to create additional accounts so that each administrator has a separate account.

There are two ways to add more manager accounts. One method adds local accounts. A local account is so called because it is the switch that authenticates the user name and password when a manager logs in. The default manager account is a local account. This chapter explains how to create more local accounts.

The switch also supports remote manager accounts. These are accounts that are authenticated by a RADIUS or TACACS+ server on your network. For information, refer to Chapter 88, "RADIUS and TACACS+ Clients" on page 1391.

Privilege Levels

Manager accounts have privilege levels that determine where in the command mode structure managers can go and, consequently, which commands they can access. The privilege levels are 1 and 15.

Manager accounts with a privilege level of 15 have access to the entire command mode structure and, thus, to all of the commands. Managers should be assigned accounts with this level if they need to configure the parameter settings of the switch. The default manager account has this privilege level.

Manager accounts with a privilege level of 1 are restricted to the User Exec mode, in which many of the SHOW commands are stored. Accounts with this level are appropriate for managers who only need to monitor the switch.

Command Mode Restriction

Command mode restriction allows you to enhance the security of the manager accounts by requiring that managers who have the privilege level 15 enter a special password to move from the User Exec mode to the Privileged Exec mode. Managers who do not know the special password are restricted to the User Exec mode, just as if their accounts had the privilege level 1.

When command mode restriction is active on the switch, managers are prompted for the special password when they enter the ENABLE command to move from the User Exec mode to the Privilege Exec mode. The prompt is shown in Figure 207 on page 1291.

```
awplus Login: adams
Password: ********




awplus> enable
Password:
```

Figure 207. Password Prompt for Command Mode Restriction

If the manager enters the correct password, the Privileged Exec mode prompt is displayed. If the wrong password or no password is entered, the manager remains in the User Exec mode, and the switch displays the error message shown in Figure 208.

```
awplus> enable
%No Local Enable Password Set
awplus>
```

Figure 208. Command Mode Restriction Error Message

The command for activating command mode restriction and defining the special password is the ENABLE PASSWORD command, in the Global Configuration mode. For instructions on how to use the command, refer to "Activating Command Mode Restriction and Creating the Special Password" on page 1296.

Command mode restriction does not apply to manager accounts with the privilege level 1. Manager accounts with that privilege level are always restricted to the User Exec mode.

Password Encryption

When you create a new manager account, you have to assign it a password. You also have to create a new password if you activate command mode restrictions. The commands for creating manager accounts and activating command mode restriction give you the choice of entering new passwords in either plaintext or encrypted form. Passwords that are entered in plaintext are stored by the switch in either plaintext or encrypted form in the running configuration and the active boot configuration file, depending on the password encryption setting. If password encryption is enabled (the default setting), plaintext passwords are stored in encrypted form. If password encryption is disabled, plaintext passwords are stored in plaintext.

Passwords entered in encrypted form when you create manager accounts, or activate command mode restriction, remain encrypted in the running configuration and the active boot configuration file, regardless of the setting of password encryption.

Password encryption is activated with the SERVICE PASSWORD-ENCRYPTION command and deactivated with the NO SERVICE PASSWORD-ENCRYPTION command, both of which are found in the Global Configuration mode. When you activate password encryption with the SERVICE PASSWORD-ENCRYPTION command, the switch searches the running configuration for plaintext passwords and encrypts them. It also automatically encrypts the plaintext passwords of new manager accounts.

When you deactivate password encryption with the NO SERVICE PASSWORD-ENCRYPTION command, the switch searches the running configuration and decrypts passwords that were initially created in plaintext.

Decrypting passwords can pose a security risk because managers can issue the NO SERVICE PASSWORD-ENCRYPTION command to see the passwords of the other accounts. To permanently encrypt passwords so that they remain in that form, even if someone issues the command, enter them in their encrypted form when you create the manager accounts or activate command mode restriction. This is illustrated in the examples in the next section.

Creating Local Manager Accounts

The command for creating local manager accounts is the USERNAME command in the Global Configuration mode. Here is the command's format:

```
username name privilege level password [8] password
```

The NAME parameter specifies the log-on name for the new account. The name is case-sensitive and can have up to 15 alphanumeric characters including special characters. Spaces are not allowed.

The LEVEL parameter specifies the privilege level of the account. The level can be either 1 or 15. Manager accounts with the privileged level 15 have access to all of the command modes, while manager accounts with the privilege level 1 are restricted to the User Exec mode.

The PASSWORD parameter specifies the password for the new manager account. You can enter the password in plaintext or encrypted. A plaintext password is case-sensitive and can have up to 16 alphanumeric characters including punctuation and printable special characters. Spaces are not permitted. To enter an encrypted password, precede it with the number '8'.

This example of the command creates an account for the user, john. The privilege level is 15 to give the manager access to the entire command mode structure. The password is "pmat762:"

```
awplus> enable
awplus# configure terminal
awplus(config)# username john privilege 15 password pmat762
```

This example creates a manager account for the user, allen. The privilege level is 1 to restrict the manager to the User Exec mode. The password for the account is "laf238pl:"

```
awplus> enable
awplus# configure terminal
awplus(config)# username allen privilege 1 password laf238pl
```

This example creates an account for the user, sjones. The privilege level is 1 to restrict the manager to the User Exec mode. The password is "bluesky," entered in its encrypted form.

```
awplus> enable
awplus# configure terminal
awplus(config)# username sjones privilege 1 password 8
c1a23116461d5856f98ee072ea319bc9
```

1293

Passwords entered in encrypted form remain encrypted in the running configuration even if you disable password encryption by issuing the NO SERVICE PASSWORD-ENCRYPTION command.

Deleting Local Manager Accounts

To delete local manager accounts from the switch, use the NO USERNAME command in the Global Configuration mode. Here is the format of the command:

```
no username name
```

The NAME parameter specifies the name of the manager account you want to delete from the switch. The name is case sensitive. You can delete just one manager account at a time with this command.

Once an account is deleted, you cannot use it to manage the switch. If you delete the account with which you logged on to the switch, your current management session is not interrupted. But you will not be able to use that account again to log in and configure the unit.

This example of the command deletes the manager account bjspring:

```
awplus> enable
awplus# configure terminal
awplus(config)# no username bjspring
```

Note
You can delete the default "manager" account from the switch.

Caution
Do not delete all of the local manager accounts that have the privilege level 15 if the switch does not have any remote RADIUS or TACACS+ accounts. Otherwise, you will not be able to log in again as manager and will have to contact Allied Telesis for assistance.

Activating Command Mode Restriction and Creating the Special Password

Command mode restriction is a security feature. It requires that managers who have the privilege level 1 enter a special password to manage the switch. The switch prompts for the special password when the ENABLE command is used to move to the Privileged Exec mode from the User Exec mode. The prompt is shown in Figure 207 on page 1291. Managers who do not know the password or have the privilege level 1 are restricted to the User Exec mode.

> **Note**
> Managers with a privilege level of 15 are only required to enter the ENABLE command to access the Privileged Exec mode and are not required to enter this password.

The command for activating command mode restriction and creating or changing the password is the ENABLE PASSWORD command in the Global Configuration mode. The switch can have only one special password. Here is the format of the command:

```
enable password [8] password
```

The PASSWORD parameter specifies the special password. You can enter the password in plaintext or encrypted. A plaintext password is case-sensitive and can have up to 16 alphanumeric characters including special characters. Spaces are not allowed. An encrypted password must be preceded by the number "8" and a space.

This example activates command mode restriction and creates the special password "Day89lane:"

```
awplus> enable
awplus# configure terminal
awplus(config)# enable password Day89lane
```

This example activates command mode restriction and specifies the password as "ship247," in encrypted form:

```
awplus> enable
awplus# configure terminal
awplus(config)# enable password 8 85076026566ed1dd84a709c0f
dd1fa9f
```

To confirm the configuration, display the running configuration with "SHOW RUNNING-CONFIG" on page 158.

Deactivating Command Mode Restriction and Deleting the Special Password

The command for deactivating command mode restriction and deleting the special password is the NO ENABLE PASSWORD command in the Global Configuration mode. When command mode restriction is deactivated, manager accounts with a privilege level of 15 do not have to enter the special password when they enter the ENABLE command to move from the User Exec mode to the Privilege Exec mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no enable password
```

Activating or Deactivating Password Encryption

Password encryption controls the manner in which the switch stores the plaintext passwords of manager accounts and command mode restriction in the running configuration. When password encryption is enabled (the default setting), plaintext passwords are stored in encrypted form. When password encryption is disabled, plaintext passwords are stored in plaintext. For more information, refer to "Password Encryption" on page 1291

To activate password encryption, issue the SERVICE PASSWORD-ENCRYPTION command in the Global Configuration mode:

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

When password encryption is activated, the switch searches the running configuration for plaintext passwords and encrypts them. It also automatically encrypts the plaintext passwords of new manager accounts.

To disable password encryption, use the NO SERVICE PASSWORD-ENCRYPTION command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service password-encryption
```

The switch searches the running configuration and decrypts passwords that were initially created in plaintext.

To keep passwords permanently encrypted, even when password encryption is disabled, create them in encrypted form when you use the USERNAME command, as explained in "Creating Local Manager Accounts" on page 1293. The switch does not decrypt passwords created in their encrypted form, even when password encryption is disabled.

Displaying the Local Manager Accounts

To view the local accounts on the switch, use "SHOW RUNNING-CONFIG" on page 158 to display the running configuration. Here is an example of several accounts.

```
username manager privilege 15 password WestWind11a
username sjones privilege 15 password Lat76rose
username smith privilege 1 password Positive89act
username adams privilege 15 password 8 c1a23116461d5856f98ee072ea319bc9
```

Figure 209. Displaying the Local Manager Accounts in the Running Configuration

Chapter 77

Local Manager Account Commands

The local manager account commands are summarized in Table 147 and described in detail within the chapter.

Table 147. Local Manager Account Commands

Command	Mode	Description
"ENABLE PASSWORD" on page 1302	Global Configuration	Activates command mode restriction on the switch and specifies the password.
"NO ENABLE PASSWORD" on page 1304	Global Configuration	Deactivates command mode restriction on the switch.
"NO SERVICE PASSWORD-ENCRYPTION" on page 1305	Global Configuration	Disables password encryption.
"NO USERNAME" on page 1306	Global Configuration	Deletes manager accounts from the switch.
"SERVICE PASSWORD-ENCRYPTION" on page 1307	Global Configuration	Encrypts all manager account passwords in the running configuration.
"USERNAME" on page 1308	Global Configuration	Creates new manager accounts.

ENABLE PASSWORD

Syntax

enable password *[8] password*

Parameters

8

Specifies that the password is encrypted.

password

Specifies the password for command mode restriction. A plaintext password is case-sensitive and can have up to 16 alphanumeric characters including special characters. Spaces are not allowed.

Mode

Global Configuration mode

Description

Use this command to activate command mode restriction on the switch and to specify the password. When command mode restriction is active, managers with a privilege level of 1 must enter the password to move to the Privileged Exec mode from the User Exec mode. Managers who do not know the password or have a privilege level of 1 are restricted to the User Exec mode.

Note
Managers with a privilege level of 15 are only required to enter the ENABLE command to access the Privileged Exec mode and are not required to enter this password.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example activates command mode restriction and specifies "wah87" as the password:

```
awplus> enable
awplus# configure terminal
awplus(config)# enable password wah87
```

This example activates command mode restriction and specifies the password as "Paperclip45c," in encrypted form:

```
awplus> enable
awplus# configure terminal
awplus(config)# enable password 8 1255bbf963118fcf750aca356d
35f6ab
```

NO ENABLE PASSWORD

Syntax

```
no enable password
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to deactivate command mode restriction on the switch to allow managers who have the privilege level 15 to access all of the command modes without having to enter the special password.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example disables command mode restriction on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no enable password
```

NO SERVICE PASSWORD-ENCRYPTION

Syntax

```
no service password-encryption
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable password encryption. The passwords of new local manager accounts are entered in clear text in the running configuration file, unless they are entered in their encrypted forms in the USERNAME command. Also, the switch decrypts all of the passwords of the current manager accounts in the running configuration file, except for passwords that were entered in their encrypted forms when the manager accounts were created.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example disables password encryption on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service password-encryption
```

NO USERNAME

Syntax

```
no username name
```

Parameters

name
> Specifies the name of the manager account you want to delete from the switch. The name is case sensitive.

Mode

Global Configuration mode

Description

Use this command to delete local manager accounts from the switch.

Note
You can delete the default "manager" account from the switch.

⚠️ **Caution**
Do not delete all of the local manager accounts that have the privilege level 15 if the switch does not have any remote RADIUS or TACACS+ accounts. Otherwise, you will not be able to log in again as manager and will have to contact Allied Telesis for assistance.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example deletes the manager account msmith:

```
awplus> enable
awplus# configure terminal
awplus(config)# no username msmith
```

SERVICE PASSWORD-ENCRYPTION

Syntax

```
service password-encryption
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate password encryption. This feature encrypts all of the manager account passwords in the running configuration of the switch and the passwords of new manager accounts. This is the default setting for password encryption.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Example

This example enables password encryption:

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

USERNAME

Syntax

username *name* privilege *level* password *[8] password*

Parameters

name

Specifies the name of a new manager account. The name is case-sensitive and can have up to 15 alphanumeric characters including special characters. Spaces are not allowed.

level

Specifies the privilege level of either 1 or 15 for the new account. Manager accounts with the privileged level 15 have access to all of the command modes, unless command mode restriction is activated. Manager accounts with the privilege level 1 are restricted to the User Exec mode.

8

Specifies that the password is encrypted.

password

Specifies the password of the new manager account. A non-encrypted password is case-sensitive and can have up to 16 alphanumeric characters including punctuation and printable special characters. Spaces are not permitted.

Mode

Global Configuration mode

Description

Use this command to create new manager accounts on the switch.

Note

Passwords for manager accounts used with the web browser interface must not be encrypted.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example creates a manager account for the user, allen. The privilege level is 15 to give the manager access to all of the modes, unless command mode restriction is activated. The password is "laf238pl:"

```
awplus> enable
awplus# configure terminal
awplus(config)# username allen privilege 15 password
laf238pl
```

This example creates a manager account for the user, sjones. The privilege level is 1 to restrict the manager to the User Exec mode. The password is "bluesky," entered in its encrypted form.

```
awplus> enable
awplus# configure terminal
awplus(config)# username sjones privilege 1 password 8
c1a23116461d5856f98ee072ea319bc9
```

1310

Chapter 78

Telnet Server

This chapter provides the following topics:

Overview

The switch comes with a Telnet server so that you can remotely manage the device from Telnet clients on your network. Remote Telnet management gives you access to the same AlliedWare Plus commands and management functions as local management sessions, which are conducted through the Console port.

The guidelines to using the Telnet server for remote management are listed here.

□ The switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

□ The management workstations with the Telnet clients must be members of the same subnet as the management IP address of the switch or have access to it through routers or other Layer 3 devices.

□ If the Telnet clients are not members of the same subnet as the switch's management IP address, the switch must have a default gateway. This is the IP address of an interface on a router or other Layer 3 routing device that is the first hop to reaching the subnets of the Telnet clients. For background information, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

□ The Telnet server uses protocol port 23. This parameter cannot be changed.

□ Telnet management sessions are not secure. The packets are sent in readable text. For secure remote management using the command line interface, use the Secure Shell protocol, described Chapter 82, "Secure Shell (SSH) Server" on page 1329.

For instructions on how to start a remote Telnet management session, refer to "Starting a Remote Telnet or SSH Management Session" on page 68.

Enabling the Telnet Server

To enable the server, go to the Global Configuration mode and issue the SERVICE TELNET command. Here is the command:

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

Once the server is started, you can conduct remote management sessions over your network from Telnet clients, provided that the switch has a management IP address. For instructions on how to start a remote Telnet management session, refer to "Starting a Remote Telnet or SSH Management Session" on page 68.

Disabling the Telnet Server

To disable the Telnet server, use the NO SERVICE TELNET command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service telnet
```
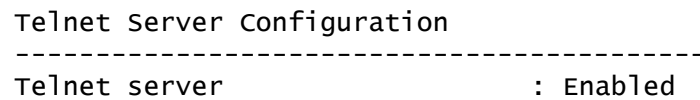
Note
If you disable the server from a remote Telnet management session, your session ends. To resume managing the unit, establish a local management session or remote web browser session. If the maximum number of manager sessions on the switch is set to one, you must wait for the console timer on the switch to expire before starting a new manager session. The default setting for the console timer is 10 minutes.

1314

Displaying the Telnet Server

To display the status of the Telnet server, use the SHOW TELNET command in the User Exec mode or Privileged Exec mode. Here is the command:

awplus# show telnet

Here is the information the command displays.

```
Telnet Server Configuration
--------------------------------------------
Telnet server                 : Enabled
```

Figure 210. SHOW TELNET Command

Chapter 79

Telnet Server Commands

The Telnet server commands are summarized in Table 148 and described in detail within the chapter.

Table 148. Telnet Server Commands

Command	Mode	Description
"NO SERVICE TELNET" on page 1318	Global Configuration	Disables the Telnet server.
"SERVICE TELNET" on page 1319	Global Configuration	Enables the Telnet server.
"SHOW TELNET" on page 1320	User Exec and Privileged Exec	Displays the status of the Telnet server on the switch.

NO SERVICE TELNET

Syntax

```
no service telnet
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the Telnet server on the switch. You cannot remotely manage the switch with a remote Telnet client when the server is disabled. The default setting for the Telnet server is enabled.

Note

Your management session ends if you disable the server from a remote Telnet session. To resume managing the unit, establish a local management session or remote web browser session. If the maximum number of manager sessions on the switch is set to one, you must wait for the console timer on the switch to expire before starting a new management session. The default setting for the console timer is 10 minutes.

Confirmation Command

"SHOW TELNET" on page 1320

Example

This example disables the Telnet server:

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

SERVICE TELNET

Syntax

```
service telnet
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the Telnet server so that you can remotely manage the switch with a Telnet application protocol. The default setting for the Telnet server is enabled.

> **Note**
> The switch must have a management IP address for remote Telnet management. For background information, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

Confirmation Command

"SHOW TELNET" on page 1320

Example

This example enables the Telnet server:

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

SHOW TELNET

Syntax

```
show telnet
```

Parameters
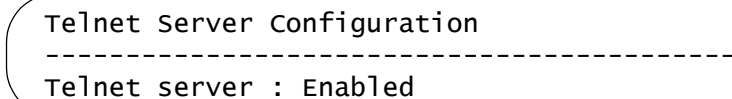
None

Mode

User Exec mode and Privileged Exec mode

Description

Use this command to display the status of the Telnet server on the switch. The status of the server can be either enabled or disabled. Here is the information.

```
Telnet Server Configuration
--------------------------------------------
Telnet server : Enabled
```

Figure 211. SHOW TELNET Command

Example

This example displays the status of the Telnet server on the switch:

```
awplus# show telnet
```

Chapter 80

Telnet Client

This chapter provides the following topics:

❏ "Overview" on page 1322

❏ "Starting a Remote Management Session with the Telnet Client" on page 1323

Overview

The switch has a Telnet client. You may use the client to remotely manage other network devices from the switch. Here are the guidelines to using the client:

❒ The client has the two commands: TELNET, which is used to manage network devices that have IPv4 addresses, and TELNET IPV6, for devices that have IPv6 addresses.

❒ You may use the Telnet client from local or Telnet management sessions of the switch, but not from remote SSH management sessions.

❒ The switch must have an IP address that is of the same type, IPv4 or IPv6, as the addresses on the remote devices. For example, the switch must have an IPv6 address for you to remotely manage devices that have IPv6 addresses. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The other network devices that you intend to manage with the Telnet client must be members of the same subnet as the IP address of the switch or have access to it through routers or other Layer 3 devices.

❒ If the other devices are not members of the same subnet as the switch's IP address, the switch must have a default gateway. This is the IP address of an interface on a router or other Layer 3 routing device that is the first hop to reaching the subnets of the devices. For background information, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ A remote device must be configured for Telnet management before you can manage it with the Telnet client on the switch. It must have either an IPv4 or IPv6 address, and its Telnet server must be active.

Starting a Remote Management Session with the Telnet Client

Here are the steps to using the Telnet client on the switch to manage other devices on your network:

1. Start a local or Telnet management session on the switch.

    > **Note**
    > The Telnet client is not supported from remote SSH management sessions.

2. If the remote device that you want to manage through the switch has an IPv4 address, move to the Privileged Exec mode and enter the TELNET command, which has this format:

    ```
    telnet ipv4_address [port]
    ```

    The IPV4_ADDRESS parameter is the IP address of the device to be managed. The optional PORT parameter is the protocol port number of the Telnet client. The default is 23. For example, if the IPv4 address of the remote device is 149.174.154.12, you enter:

    ```
    awplus> enable
    awplus# telnet 149.174.154.12
    ```

    You should now see the login prompts of the remote device.

3. If the remote device to be managed has an IPv6 address, move to the Privileged Exec mode and enter the TELNET IPV6 command, which has this format:

    ```
    telnet ipv6 ipv6_address [port]
    ```

    The IPV6_ADDRESS parameter is the IP address of the device to be managed. For example, if the remote device had the IPv6 address 45ac:be45:78::c45:8156, you enter:

    ```
    awplus> enable
    awplus# telnet ipv6 45ac:be45:78::c45:8156
    ```

    You should now see the login prompts of the remote device.

4. Enter the appropriate user name and password for the remote device.

5. When you finish managing the remote device, enter the appropriate logout command to return to the management session on the AT-9000 Switch.

1323

1324

Chapter 81
Telnet Client Commands

The Telnet client commands are summarized in Table 149 and described in detail within the chapter.

Table 149. Telnet Client Commands

Command	Mode	Description
"TELNET" on page 1326	Privileged Exec	Starts Telnet management sessions on remote devices that have IPv4 addresses.
"TELNET IPV6" on page 1327	Privileged Exec	Starts Telnet management sessions on remote devices that have IPv6 addresses.

TELNET

Syntax

```
telnet ipv4_address [port]
```

Parameters

ipv4_address
>   Specifies the IPv4 address of a remote device you want to manage
>   using the Telnet client on the switch. You can specify just one
>   address.

port
>   Specifies the protocol port number of the Telnet client. The default
>   value is 23.

Mode

Privileged Exec mode

Description

Use this command to start Telnet management sessions on network
devices that have IPv4 addresses. You can manage just one remote
device at a time.

Note
This command is available from local and Telnet management
sessions.

Example

This example starts a Telnet management session on a network device
that has the IP address 132.154.67.134:

```
awplus> enable
awplus# telnet 132.154.67.134
```

TELNET IPV6

Syntax

```
telnet ipv6 ipv6_address [port]
```

Parameters

ipv6_address
> Specifies the IPv6 address of a remote device you want to manage using the Telnet client on the switch. You can specify just one address.

port
> Specifies the protocol port number of the Telnet client. The default value is 23.

Mode

Privileged Exec mode

Description

Use this command to start Telnet management sessions on network devices that have IPv6 addresses. You can manage just one remote device at a time.

> **Note**
> This command is available from local and Telnet management sessions, but not from SSH management sessions.

Example

This example starts a Telnet management session on a network device that has the IPv6 address 45ac:be45:78::c45:8156:

```
awplus> enable
awplus# telnet ipv6 45ac:be45:78::c45:8156
```

Chapter 82

Secure Shell (SSH) Server

This chapter provides the following topics:

Overview

The Secure Shell (SSH) protocol is an alternative to the Telnet protocol for remote management of the switch from workstations on your network. The difference between the two management methods is that SSH management is more secure because the packets the switch and your management workstation exchange during management sessions are encrypted. In contrast, Telnet management sessions are unsecured and are vulnerable to snooping because the packets are sent in readable text.

The SSH server on the switch supports SSH protocol versions 1.3, 1.5, and 2.0. Client software is available on the Internet.

Algorithms
The SSH server on the switch encrypts the packets using an encryption key. The key is created with an algorithm. You can choose from three available algorithms to create the key for SSH:

- ❐ RSA
- ❐ RSA1
- ❐ DSA

Support for SSH

The implementation of the SSH protocol on the switch is compliant with the SSH protocol versions 1.3, 1.5, and 2.0.

In addition, the following SSH options and features are supported:

❒ Inbound SSH connections (server mode) is supported.

❒ The following security algorithms are supported:

– 128-bit Advanced Encryption Standard (AES), 192-bit AES, and 256-bit AES

– Arcfour (RC4) security algorithm is supported.

– Triple-DES (3DES) encryption for SSH sessions is supported.

❒ RSA public keys with lengths of 768 to 2048 bits are supported. Keys are stored in a format compatible with other Secure Shell implementations.

❒ Compression of SSH traffic.

❒ The switch uses the well-known port 22 as the SSH default port.

The following SSH options and features are **not** supported:

❒ IDEA or Blowfish encryption

❒ Non-encrypted Secure Shell sessions

❒ Tunnelling of TCP/IP traffic

Guidelines

Here are the guidelines to using SSH to manage the switch:

❒ The switch must have a management IP address. For background information, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The management workstations with the SSH clients must be members of the same subnet as the management IP address of the switch or have access to it through routers or other Layer 3 devices.

❒ If the SSH clients are not members of the same subnet as the switch's management IP address, the switch must have a default gateway. This is the IP address of an interface on a router or other Layer 3 routing device that is the first hop to reaching the subnets of the Telnet clients. For background information, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ The SSH server uses protocol port 22. This parameter cannot be changed.

❐ If you are using the enhanced stacking feature, you activate and configure SSH server on the master switch, not on the member switches.

Note
If your switch is in a network that is protected by a firewall, you may need to configure the firewall to permit SSH connections.

For instructions on how to start a remote management session, refer to "Starting a Remote Telnet or SSH Management Session" on page 68.

SSH and Enhanced Stacking

The switch allows for encrypted SSH management sessions between a management station and the master switch of an enhanced stack, but not with member switches, as explained in this section.

When you remotely manage a member switch, all management communications are conducted through the master switch using the enhanced stacking feature. Management packets from your workstation are first directed to the master switch before being forwarded to the member switch. The reverse is true as well. Management packets from a member switch first pass through the master switch before reaching your management station.

Enhanced stacking uses a proprietary protocol different from Telnet and SSH protocols. Consequently, there is no encryption between a master switch and a member switch. The result is that SSH encryption only occurs between your workstation and the master switch, not between your workstation and a member switch.

This is illustrated in Figure 212. The figure shows an SSH management station that is managing a member switch of an enhanced stack. The packets exchanged between the member switch and the master switch are transmitted in plaintext and those exchanged between the master switch and the SSH management station are encrypted.

Member Switch

Plaintext Management Packets
(Proprietary Enhanced Stacking Protocol)

Command Switch

Encrypted Management Packets
(SSH Protocol)

SSH
Management
Workstation
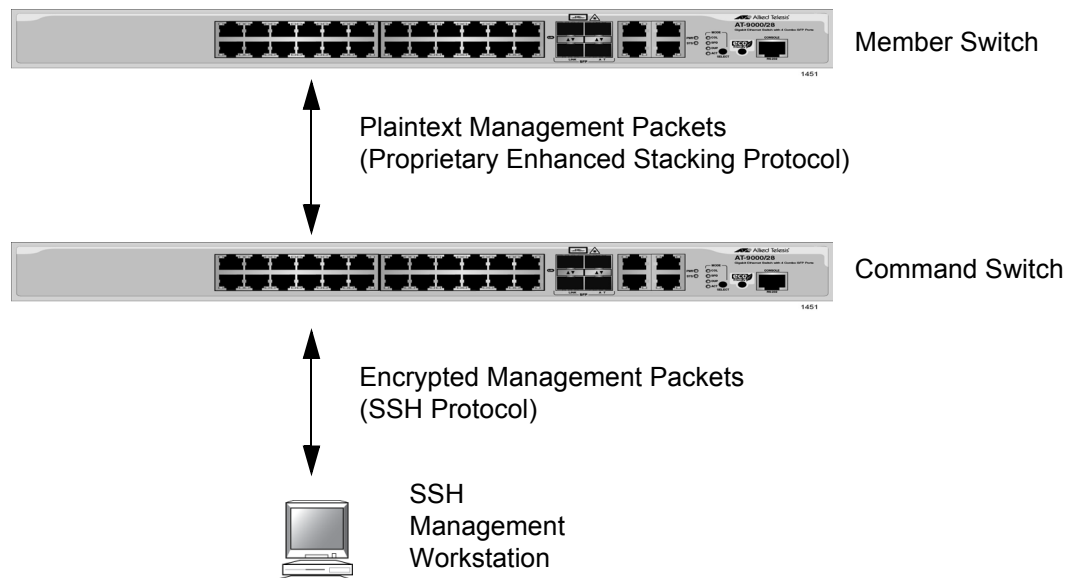
Figure 212. SSH Remote Management of a Member Switch

Because enhanced stacking does not allow for SSH encrypted management sessions between a management station and a member switch, you configure SSH only on the master switch of a stack. Activating SSH on a member switch has no effect.

Creating the Encryption Key Pair

The first step to using the SSH server on the switch for remote management is to create the encryption key. Here is the base command:

```
crypto key generate hostkey dsa|rsa|rsa1 [value]
```

The VALUE parameter only applies to an RSA key.

To create a DSA key, enter these commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey dsa
```

To create an RSA1 key, enter these commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa1
```

An RSA key is different from the other keys because you can specify a length in bits by using the VALUE parameter in the command. The other keys have a fixed key length of 1024 bits. The range is 768 to 2048 bits. Entering the length is optional. This example creates an RSA key with a length of 768 bits:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 768
```

DSA and RSA1 keys take less than a minute to create. An RSA key that has the maximum key length of 2048 bits may take as much as four minutes for the switch to create.

> **Note**
> Creating a key is a very CPU intensive process for the switch. The switch does not stop forwarding network packets, but it may delay handling some network events, such as spanning tree BPDU packets. To avoid unexpected or unwanted switch behavior, create a key during periods of low network activity.

Enabling the SSH Server

The switch does not allow you to enable the SSH server and begin remote management until you have created the encryption key. So if you have not done that yet, perform the instructions in the previous procedure.

The command that activates the server is the SERVICE SSH command in the Global Configuration mode. Here is the command:

```
awplus> enable
awplus# configure terminal
awplus(config)# service ssh
```

After you enter the command, the switch searches its database for an encryption key. If it finds a key, it immediately enables the server. Otherwise, it does not activate the server.

With the server activated, you can begin to manage the switch remotely from SSH clients on your network.

1336

Disabling the SSH Server

If you decide that you want to disable the server because you do not want to remotely manage the switch with SSH, enter the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service ssh
```

Note
If you disable the server during a remote SSH management session, your session ends. To resume managing the unit with the same management account, you must wait for the console timer on the switch to expire and then establish a local management session or remote Telnet or web browser session.

Deleting Encryption Keys

To delete encryption keys from the switch, use the CRYPTO KEY DESTROY HOSTKEY command in the Global Configuration mode. Here is the format of the command:

```
crypto key destroy hostkey dsa|rsa|rsa1
```

> **Note**
> You should disable the SSH server before deleting the encryption key. The operations of the server will be impaired if you delete the active key when the server is enabled.

> **Note**
> If you disable the server during a remote SSH management session, your session ends. To resume managing the unit with the manager account, you must wait for the console timer on the switch to expire and then establish a local management session or remote Telnet or web browser session.

This example deletes the DSA key:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service ssh
awplus(config)# crypto key destroy hostkey dsa
```

This example deletes the RSA key:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service ssh
awplus(config)# crypto key destroy hostkey rsa
```

This example deletes the RSA1 key:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service ssh
awplus(config)# crypto key destroy hostkey rsa1
```

Displaying the SSH Server

To display the current settings of the server, enter this command in the Privileged Exec or Global Configuration mode:

```
awplus# show ssh server
```

Chapter 83
SSH Server Commands

The SSH server commands are summarized in Table 150 and described in detail within the chapter.

Table 150. Secure Shell Server Commands

Command	Mode	Description
"CRYPTO KEY DESTROY HOSTKEY" on page 1342	Global Configuration	Deletes encryption keys from the switch.
"CRYPTO KEY GENERATE HOSTKEY" on page 1344	Global Configuration	Creates encryption keys.
"NO SERVICE SSH" on page 1346	Global Configuration	Disables the SSH server.
"SERVICE SSH" on page 1347	Global Configuration	Activates the SSH server and specifies the host and server encryption keys.
"SHOW CRYPTO KEY HOSTKEY" on page 1348	Privileged and Global Configuration	Displays the encryption keys.
"SHOW SSH SERVER" on page 1349	Privileged and Global Configuration	Displays the parameter settings of the SSH server.

1341

CRYPTO KEY DESTROY HOSTKEY

Syntax

```
crypto key destroy hostkey dsa|rsa|rsa1
```

Parameters

dsa

Deletes the DSA key.

rsa

Deletes the RSA key.

rsa1

Deletes the RSA1 key.

Mode

Global Configuration mode

Description

Use this command to delete encryption keys from the switch. Deleted encryption keys are permanently removed by the switch when you enter this command. You do not have to enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command to save your changes on the switch.

Confirmation Command

"SHOW CRYPTO KEY HOSTKEY" on page 1348

Examples

This example deletes the DSA key:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key destroy hostkey dsa
```

This example deletes the RSA key:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

This example deletes the RSA1 key:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa1
```

CRYPTO KEY GENERATE HOSTKEY

Syntax

```
crypto key generate hostkey dsa/rsa/rsa1 [value]
```

Parameters

dsa

Creates a DSA key that is compatible with SSH versions 1 and 2.

rsa

Creates an RSA key that is compatible with SSH version 2.

rsa1

Creates an RSA key that is compatible with SSH version 1.

value

Specifies the length of the encryption key in bits. The length is specified only for an RSA key and is optional. The range is 768 to 2048 bits. DSA and RSA1 keys have fixed lengths of 1024 bits.

Mode

Global Configuration mode

Confirmation Command

"SHOW CRYPTO KEY HOSTKEY" on page 1348

Description

Use this command to create the encryption key for the Secure Shell server. You must create the key before activating the server. The switch can have one key of each type at the same time.

If you create a new key when the switch already has a key of that type, the new key overwrites the old key. For example, if you create a new RSA key when the switch already has an RSA key, the new key replaces the existing key.

A new encryption key is automatically saved by the switch when you enter the command. You do not have to enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command to save your changes on the switch.

DSA and RSA1 keys take less than a minute to create. However, an RSA key that has the maximum key length of 2048 bits may take as much as four minutes for the switch to create.

1344

> **Note**
> Creating a key is a very CPU intensive process for the switch. The switch does not stop forwarding network packets, but it may delay handling some network events, such as spanning tree BPDU packets. To avoid unexpected or unwanted switch behavior, create a key during periods of low network activity.

Examples

This example creates a DSA key:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey dsa
```

This example creates an RSA key with a length of 1280 bits:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 1280
```

This example creates an RSA1 key:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa1
```

NO SERVICE SSH

Syntax

```
no service ssh
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the Secure Shell server to prevent remote management of the switch using a Secure Shell client. The default setting for the Secure Shell server is disabled.

Note
Your management session of the switch ends if you disable the server from a remote SSH management session. To resume managing the switch from a local management session or a remote Telnet or web browser session, you must wait for the console timer to expire if the switch is configured to support one manager session at a time. The default setting for the console timer is 10 minutes.

Confirmation Command

"SHOW SSH SERVER" on page 1349

Example

This example disables the Secure Shell server:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service ssh
```

SERVICE SSH

Syntax

```
service ssh
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the Secure Shell server on the switch.

You must create an encryption key before enabling the server. For instructions, refer to "CRYPTO KEY GENERATE HOSTKEY" on page 1344.

Confirmation Command

"SHOW SSH SERVER" on page 1349

Example

This example enables the Secure Shell server on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# service ssh
```

SHOW CRYPTO KEY HOSTKEY

Syntax

```
show crypto key hostkey [dsa/rsa/rsa1]
```

Parameters

dsa

Displays the DSA key.

rsa

Displays the RSA key.

rsa1

Displays the RSA1 key.

Mode

Global Configuration mode

Description

Use this command to display the encryption keys. Here is an example of the information for an RSA key.

```
Type   Bits   Fingerprint
-------------------------------------------------------------
RSA    1280   60:59:ff:78:e7:4e:58:24:e6:57:bc:c9:d1:c9:73:91
```

Figure 213. SHOW CRYPTO KEY HOSTKEY Command

Examples

This example displays all of the keys:

```
awplus# show crypto key hostkey
```

This example displays the RSA1 key only:

```
awplus# show crypto key hostkey rsa1
```

SHOW SSH SERVER

Syntax

show ssh server

Parameters

None

Modes

Privileged Exec and Global Configuration modes

Description

Use this command to display the current status of the SSH server.

❒ Versions supported

❒ Server Status

❒ Server Port

Example

This example displays the status of the SSH server:

awplus# show ssh server

An example of the information the command displays is shown in Figure 214.

```
Secure Shell Server Configuration
Versions Supported ........ 2,1
SSH Server :   Enabled
Server Port .............. 22
```

Figure 214. SHOW SSH SERVER Command

Chapter 84

Non-secure HTTP Web Browser Server

This chapter describes the following topics:

Overview

The switch has a web browser server. The server is used to remotely manage the unit over the network with web browser applications. The server can operate in either plain text HTTP mode or encrypted HTTPS mode. This chapter explains how to activate the server for the HTTP mode.

⚠️ **Caution**

Management sessions of the switch conducted in the HTTP mode are non-secure because the packets exchanged by your web browser application and the server on the switch are sent in clear text, leaving them vulnerable to snooping. If an individual captures the management packet that contains your user name and password, he or she could use that information to access the switch and make unauthorized changes to its configuration settings.

Here are the guidelines to using the web browser server in the non-secure HTTP mode:

❒ The switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The management workstations from which you will configure the switch with web browser applications must be members of the same network as the management IP address of the switch, or they must have access to it through routers or other Layer 3 devices.

❒ The web browser server cannot operate in both HTTP mode and HTTPS mode at the same time.

❒ The switch supports the HTTP v1.0 and v1.1 protocols.

Enabling the Web Browser Server

The command to activate the web browser server for non-secure HTTP operation is the SERVICE HTTP command in the Global Configuration mode. The command, which does not have any parameters, is shown here:

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

Here are the guidelines to using the command:

❒ The switch should already have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ If the web browser server is already configured for secure HTTPS, and you are changing it back to non-secure HTTP operation, you must first deactivate the HTTPS server with the NO SERVICE HTTPS command, also in the Global Configuration mode.

Now that the server is activated for HTTP operation, you can begin to manage the switch remotely using a web browser application from a workstation on your network. Enter the IP address of the switch in the URL field of the application and, when prompted by the switch, enter your login user name and password.

Setting the Protocol Port Number

The default setting of port 80 for the protocol port of the HTTP web server can be adjusted with the IP HTTP PORT command in the Global Configuration mode. This example of the command changes the protocol port to 100:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip http port 100
```

The range of the port number is 0 to 65535.

Disabling the Web Browser Server

The command to disable the HTTP server is the NO SERVICE HTTP command in the Global Configuration mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service http
```
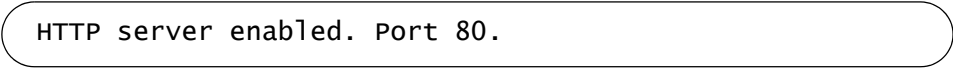
No further web browser management sessions are permitted by the switch after the server is disabled. Any web browser sessions that are in progress when the server is disabled are interrupted and are not allowed to continue.

Displaying the Web Browser Server

To display whether the HTTP web server is enabled or disabled on the switch, issue the SHOW IP HTTP command in the Privileged Exec mode. The command also displays the protocol port number if the server is enabled. Here is the command:

```
awplus> enable
awplus# show ip http
```

Here is an example of the display.

```
HTTP server enabled. Port 80.
```

Figure 215. SHOW IP HTTP Command

Chapter 85

Non-secure HTTP Web Browser Server Commands

The non-secure HTTP web browser server commands are summarized in Table 151 and described in detail within the chapter.

Table 151. Non-secure HTTP Web Browser Server Commands

Command	Mode	Description
"SERVICE HTTP" on page 1358	Global Configuration	Enables the HTTP web browser server.
"IP HTTP PORT" on page 1359	Global Configuration	Sets the protocol port number of the server.
"NO SERVICE HTTP" on page 1360	Global Configuration	Disables the web browser server.
"SHOW IP HTTP" on page 1361	Privileged Exec	Displays the settings of the server.

SERVICE HTTP

Syntax

```
service http
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the HTTP web browser server on the switch. The switch supports non-secure HTTP web browser management sessions when the server is activated.

Confirmation Command

"SHOW IP HTTP" on page 1361.

Example

This example activates the HTTP web browser server on the switch:

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

IP HTTP PORT

Syntax

```
ip http port port
```

Parameters

port

Specifies the TCP port number the HTTP web server listens on. The range is 0 to 65535.

Mode

Global Configuration mode

Description

Use this command to set the TCP port for the web browser server.

Confirmation Command

"SHOW IP HTTP" on page 1361

Example

This examples sets the TCP port for the HTTP server to 74:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip http port 74
```

NO SERVICE HTTP

Syntax

```
no http server
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the HTTP web browser server on the switch to prevent any further remote management with a web browser. Any active web browser management session are interrupted and are not allowed to continue. You might disable the server to prevent remote web browser management sessions of the switch or in prelude to activating the secure HTTPS web browser server.

Confirmation Command

"SHOW IP HTTP" on page 1361.

Example

This example disables the HTTP web browser server on the switch:

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

SHOW IP HTTP

Syntax

```
show ip http
```
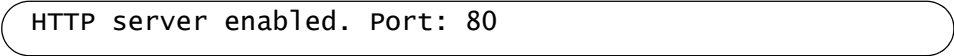
Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the status of the HTTP server on the switch. Here is an example of the information.

```
HTTP server enabled. Port: 80
```

Figure 216. SHOW IP HTTP Command

Example

This example display the status of the HTTP server on the switch:

```
awplus# show ip http
```

Chapter 86

Secure HTTPS Web Browser Server

This chapter describes the following topics:

1363

Overview

The switch has a web browser server for remote management of the unit with a web browser application from management workstations on your network. The server has a secure HTTPS mode and a non-secure HTTP mode. Web browser management sessions that use the secure HTTPS mode are protected against snooping because the packets exchanged between the switch and your management workstations are encrypted. Only the switch and the workstations are able to decipher the packets.

In contrast, web browser management sessions conducted in the non-secure HTTP mode are vulnerable to eavesdropping because the packets are sent in clear text.

This chapter explains how to configure the switch for the secure HTTPS mode. For directions on the non-secure mode, refer to Chapter 84, "Non-secure HTTP Web Browser Server" on page 1351.

Certificates   When you initiate an HTTPS connection from your management workstation to the switch, the switch responds by sending a certificate to your workstation. This file contains the encryption key that the two devices use to encrypt and decrypt their packets to each other. Also included in the certificate is a distinguished name that identifies the owner of the certificate, which in the case of a certificate for your switch, is the switch itself and your company.

The switch does not come with a certificate. You have to create it, along with the encryption key and distinguished name, as part of the HTTPS configuration process.

There are two ways to create the certificate. The quickest and easiest way is to have the switch create it itself. This type of certificate is called a self-signed certificate because the switch authenticates the certificate itself.

Another option is to create the encryption key and have someone else issue the certificate. That person, group, or organization is called a certification authority (CA), of which there are public and private CAs. A public CA issues certificates typically intended for use by the general public, for other companies or organizations. Public CAs require proof of the identify of the company or organization before they will issue a certificate. VeriSign is an example of a public CA.

Because the certificate for the switch is not intended for general use and will only be used by you and other network managers to manage the device, having a public CA issue the certificate will probably be unnecessary.

Some large companies have private CAs. This is a person or group that is responsible for issuing certificates for the company's network equipment.

Private CAs allow companies to keep track of the certificates and control access to various network devices.

If your company is large enough, it might have a private CA, and you might want that group to issue the certificate for the switch so that you are in compliance with company policy.

If you choose to have a public or private CA issue the certificate, you must first create a self-signed certificate. Afterwards, you have to generate a digital document, called an enrollment request, which you send to the CA. The document contains the public key and other information that the CA will use to create the certificate.

Before sending an enrollment request to a CA, you should contact the CA to determine what other documents or procedures might be required in order for the CA to process the certificate. This is particularly important with public CAs, which typically have strict guidelines on issuing certificates.

Distinguished Name

A certificate, whether its self-signed by the switch or issued by a CA, must identity its owner, which, in the case of a certificate for the switch, is the switch itself and your company. The name of the owner is entered in the form of a distinguished name, which has six parts.

- ❒ Common name (cn): This is the IP address or name of the switch.
- ❒ Organizational unit (ou): This is the name of the department, such as Network Support or IT, that the switch is serving.
- ❒ Organization (o): This is the name of your company.
- ❒ Location: The location of the switch or company, such as the city.
- ❒ State (st): The state where the switch or company is located.
- ❒ Country (c): This is the country.

The common name of a certificate for the switch should be its IP address.

At the start of an HTTPS web browser management session with the switch, the web browser on your management station checks to see if the name to whom the certificate was issued matches the name of the web site. In the case of the switch, the web site's name is the switch's IP address. If they do not match, your web browser displays a security warning. It is for this reason that the common name in the distinguished name should be the IP address of the switch. Of course, even if you see the security warning, you can close the warning prompt and still configure the switch using your web browser.

Alternatively, if your network has a Domain Name System, and you mapped a name to the IP address of the switch, you can specify the switch's name, instead of the IP address as the common name in the distinguished name.

> **Note**
> If the certificate will be issued by a private or public CA, you should check with the CA to see if they have any rules or guidelines on distinguished names for the certificates they issue.

Guidelines

The guidelines for creating certificates are:

❐ The switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ The management workstations from which you will configure the switch with web browser applications must be members of the same network as the management IP address of the switch, or they must have access to it through routers or other Layer 3 devices.

❐ The web browser server cannot operate in both HTTP mode and HTTPS mode at the same time.

❐ A certificate can have only one encryption key.

❐ The switch can use only certificates containing keys that it generated.

❐ The switch can have up to eight certificates, but only one can be active at a time.

❐ Your web browser must support HTTPS to use encryption.

❐ The switch supports HTTPS v1.0 and v1.1 protocols running over SSL.

❐ The switch supports RSA encryption.

The switch supports the following SSL protocols:

❐ SSL version 2.0

❐ SSL version 3.0

❐ TLS (Transmission Layer Security) version 1.0

1366

Creating a Self-signed Certificate

Here are the main steps to configuring the switch for a self-signed certificate:

1. Create a new self-signed certificate with "CRYPTO CERTIFICATE GENERATE" on page 1379, in the Global Configuration mode. The command has this format:

   ```
   crypto certificate id_number generate length passphrase
   common_name organizational_unit organization location
   state country duration
   ```

   The ID_NUMBER parameter is a value from 1 to 10 that uniquely identifies the certificate on the switch. Since the switch cannot have more than eight certificates, and since only one certificate can be active at a time, you probably will not create more than one or two certificates.

   The length specifies the length in bits of the encryption key of the certificate. The range is 512 to 1536 bits.

   The PASSPHRASE parameter consists of 4 to 20 alphanumeric characters that are used to export the certificate in PKCS12 file format. Although the switch does not allow you to export certificates, you are still required to include a value for this parameter in the command.

   The COMMON_NAME, ORGANIZATIONAL_UNIT, ORGANIZATION, LOCATION, STATE, and COUNTRY parameters make up the distinguished name of the certificate. All of these parameters, with the exception of the COUNTRY parameter, have lengths up to 64 characters. Spaces and special characters are not allowed.

   The COUNTRY parameter is the two-character ISO 3166-1 initials of the country, in uppercase letters.

2. After creating the self-signed certificate, designate it as the active certificate on the switch with "IP HTTPS CERTIFICATE" on page 1386, in the Global Configuration mode. The command has this format:

   ```
   ip https certificate id_number
   ```

   The ID_NUMBER parameter is the ID number of the new certificate you created in Step 1.

3. Activate the HTTPS web browser server with "SERVICE HTTPS" on page 1385, in the Global Configuration mode. This command has no parameters.

At this point, the switch, if it has a management IP address, is ready for remote management with a web browser application. To start a management session, enter the IP address of the switch in the URL field of your web browser, being sure to include the prefix "https://".

Here is an example of how to create a self-signed certificate and how to configure the HTTPS web browser server for the certificate. The specifications of the certificate are listed here:

- ID number: 2
- Key length: 1280
- Passphrase: trailtree
- Common name: 167.214.121.45 (This is the IP address of the switch.)
- Organizational unit: Sales
- Organization: Jones_Industries
- Location: San_Jose
- State: California
- Country: US
- Duration: 365 days

`awplus> enable`	Enter the Privileged Exec mode from the User Exec mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# crypto certificate 2 generate 1280 trailtree 167.214.121.45 Sales Jones_Industries San_Jose California US 365`	Create the self-signed certificate with "CRYPTO CERTIFICATE GENERATE" on page 1379.

`Generating a 1280 bit RSA private key`
`.......................................+++++`
`.................................+++++`
`writing new private key to '/cfg/cert2.pem'`
	Here is what the switch displays as it creates the certificate.

`awplus(config)# ip https certificate 2`	Designate the new certificate as the active certificate on the switch with "IP HTTPS CERTIFICATE" on page 1386.
`awplus(config)# no http server`	If the non-secure HTTP web browser server is enabled on the unit, disabled it with "NO SERVICE HTTP" on page 1360.

awplus(config)# service https	Enable the HTTPS server with "SERVICE HTTPS" on page 1385.
awplus(config)# exit	Return to the Privileged Exec mode.
awplus# show ip https	Confirm the confirmation with "SHOW IP HTTPS" on page 1389.

```
HTTPS server enabled. Port: 443
Certificate 2 is active
Issued by: self-signed
Valid from: 1/1/2000 to 12/31/2000
Subject: C=US, ST=California, L=San_Jose, O=Jones_Industries, OU=Sales,
CN=167.214.121.45
Finger print: FBFBAA5F 2673E463 E784F1C1 A3717881
```

The switch is now ready for remote web browser management with HTTPS, provided that it has a management IP address.

Configuring the HTTPS Web Server for a Certificate Issued by a CA

Here are the main steps to configuring the HTTPS web browser server for a certificate from a CA:

1. Create a self-signed certificate with "CRYPTO CERTIFICATE GENERATE" on page 1379, in the Global Configuration mode. The command has this format:

   ```
   crypto certificate id_number generate length passphrase
   common_name organizational_unit organization location
   state country duration
   ```

   The parameters are described in Step 1 in the previous procedure and in "CRYPTO CERTIFICATE GENERATE" on page 1379.

2. Create an enrollment request with "CRYPTO CERTIFICATE REQUEST" on page 1383, in the Global Configuration mode. The format of the command is shown here:

   ```
   crypto certificate id_number request common_name
   organizational_unit organization location state country
   ```

   The values of the parameters in this command must be exactly the same as the corresponding values from the CRYPTO CERTIFICATE GENERATE command, used to create the self-signed certificate. This includes the ID_NUMBER parameter. Any differences, including differences in capitalizations, will cause the switch to reject the CA certificate when you import it into the switch's certificate database.

3. Cut and paste the enrollment request from your screen into a word processor document.

4. Submit the enrollment request to the CA.

5. After you receive the certificate files from the CA, download them into the switch's file system using TFTP or Zmodem. For instructions, refer to Chapter 30, "File Transfer" on page 489. Be sure to download all certificate files from the CA.

6. Import the certificate into the certificate database with "CRYPTO CERTIFICATE IMPORT" on page 1382. The command has this format:

   ```
   crypto certificate id_number import
   ```

   The ID_NUMBER parameter is the ID number you assigned the self-signed certificate and enrollment request.

7. Designate the new certificate from the CA as the active certificate on the switch with "IP HTTPS CERTIFICATE" on page 1386, in the Global Configuration mode. The command has this format:

    ip https certificate *id_number*

    The ID_NUMBER parameter is the ID number you assigned the self-signed certificate and enrollment request.

8. Activate the HTTPS web browser server with "SERVICE HTTPS" on page 1385, in the Global Configuration mode. This command has no parameters.

Here is an example of how to configure the HTTPS web browser server for a certificate from a public or private CA. The certificate is assigned these specifications:

- ❏ ID number: 1
- ❏ Key length: 512
- ❏ Passphrase: hazeltime
- ❏ Common name: 124.201.76.54 (This is the IP address of the switch.)
- ❏ Organizational unit: Production
- ❏ Organization: ABC_Industries
- ❏ Location: San_Jose
- ❏ State: California
- ❏ Country: US
- ❏ Duration: 365 days

`awplus> enable`	Enter the Privileged Exec mode from the User Exec mode.
`awplus# configure terminal`	Enter the Global Configuration mode.
`awplus(config)# crypto certificate 1 generate 512 hazeltime 124.201.76.54 Production ABC_Industries San_Jose California US 365`	Create the self-signed certificate with "CRYPTO CERTIFICATE GENERATE" on page 1379.

`Generating a 512 bit RSA private key`
`......................................++++`
`...................................++++`
`writing new private key to '/cfg/cer1.pem'`
	This is the information the switch displays as it creates the certificate.

1371

awplus(config)# crypto certificate 1 request 124.201.76.54 Production ABC_Industries San_Jose California US	Create an enrollment request that has exactly the same information, including the same ID number, as the self-signed certificate, with "CRYPTO CERTIFICATE REQUEST" on page 1383.
	Cut and paste the certificate request from your screen into a word processor document.

```
-----BEGIN CERTIFICATE REQUEST-----

MIIBuzCCASQCAQAwezELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx
ETAPBgNVBAcUCFNhbl9Kb3NlMRcwFQYDVQQKFA5BQkNfSW5kdXN0cmllczETMBEG
A1UECxMKUHJvZHVjdGlvbjEWMBQGA1UEAxMNMTI0LjIwMS43Ni41NDCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAs4BrmXN3IEdOvyMEwE3DXLxl77NMKjy1OIDU
PYGJK6DuP2M+fk1sBMG/gjFIeMldmWl2HcILehGU9lCRtjqsOXLp4yVj1D8CmrPM
ipnu7UhYWD8T7hF9y7sGfxOKhzSc7x1pOkiZzfi/nQZ89TYwn9hxPMCTtpY+iBCH
IXAXXW8CAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBACmW6H1yRWUrbPn2J8B2ygFP
DZ42gjNOpJdfK94vmS7Kv/VZpFHxakjLjSiXlDaUbqmqceG+JtBnOyEPO+Xr/WBl
llyf9tr29O/temY9iD+U2E9PVdl6mKgOsB+762Ys1kqNy7S79SS9grMnPmbO+rvH
ipN2U4jKPOZHOrIrdxaN

-----END CERTIFICATE REQUEST-----
```

-	Submit the request, along with any other necessary information, to the public or private CA.
-	After receiving the certificate from the CA, download it into the switch's file system, with TFTP or Zmodem. Be sure to download all the certificate files from the CA. For instructions, refer to Chapter 30, "File Transfer" on page 489.
awplus(config)# crypto certificate 1 import	Import the new certificate into the certificate database with "CRYPTO CERTIFICATE IMPORT" on page 1382.
awplus(config)# ip https certificate 1	Designate the new certificate as the active certificate on the switch with "IP HTTPS CERTIFICATE" on page 1386.

awplus(config)# no http server	If the non-secure HTTP web browser server is enabled on the unit, disabled it with "NO SERVICE HTTP" on page 1360.
awplus(config)# service https	Enable the HTTPS server with "SERVICE HTTPS" on page 1385.
awplus(config)# exit	Return to the Privileged Exec mode.
awplus# show ip https	Confirm the confirmation with "SHOW IP HTTPS" on page 1389.

```
HTTPS server enabled. Port: 443
Certificate 1 active
Issued by: ABC_Industries_IT
Valid from: 1/1/2000 to 12/31/2000
Subject: C=US, ST=California, L=San_Jose, O=ABC_Industries,
OU=Production, CN=124.201.76.54
Finger print: FBFBAA5F 2673E463 E784F1C1 A3717881
```

The switch, if it has a management IP address, is now ready for remote HTTPS web browser management. To start a management session, enter the IP address of the switch in the URL field of your web browser, being sure to include the prefix "https://".

Enabling the Web Browser Server

The command to activate the web browser server for secure HTTPS operation is the SERVICE HTTPS command in the Global Configuration mode. The command, which does not have any parameters, is shown here:

```
awplus> enable
awplus# configure terminal
awplus(config)# service https
```

Here are the guidelines to the command:

❐ The switch should already have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❐ The switch should have a HTTPS certificate.

❐ If the HTTP mode is enabled, you must disable it with the NO HTTP SERVER command before activating the HTTPS mode. The command is in the Global Configuration mode.

Now that the server is activated for HTTPS operation, you can begin to manage the switch remotely using a web browser application from a workstation on your network. Enter the IP address of the switch in the URL field of the application and, when prompted by the switch, enter your login user name and password. Be sure to include the "HTTPS://" prefix with the IP address.

Disabling the Web Browser Server

The command to disable the HTTPS mode is the NO SERVICE HTTPS command in the Global Configuration mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service https
```

No further web browser management sessions are permitted by the switch after the server is disabled. Any web browser sessions that are in progress when the server is disabled are interrupted and are not allowed to continue.

Displaying the Web Browser Server

To display whether the HTTPS web server is enabled or disabled on the switch, issue the SHOW IP HTTPS command in the Privileged Exec mode. The command also displays the protocol port number if the server is enabled. Here is the command:

```
awplus> enable
awplus# show ip https
```

Here is an example of the display.

```
HTTPS server enabled. Port: 443
Certificate 1 is active
Issued by: self-signed
Valid from: 5/17/2010 to 5/16/2011
Subject: C=US, ST=California, L=San_Jose, O=ABC_Inc, OU=Production,
CN=169.254.143.1
Finger print: 5C7D34A9 5283B3C 87901271 6C66D2F5
```

Figure 217. SHOW IP HTTPS Command

The fields are described in Table 153 on page 1389.

Chapter 87

Secure HTTPS Web Browser Server Commands

The secure HTTPS web browser server commands are summarized in Table 152 and described in detail within the chapter.

Table 152. Secure HTTPS Web Browser Server Commands

Command	Mode	Description
"CRYPTO CERTIFICATE DESTROY" on page 1378	Global Configuration	Deletes unused certificates from the switch.
"CRYPTO CERTIFICATE GENERATE" on page 1379	Global Configuration	Creates self-signed certificates for secure HTTPS web browser management of the switch.
"CRYPTO CERTIFICATE IMPORT" on page 1382	Global Configuration	Imports certificates from public or private CAs into the certificate database on the switch.
"CRYPTO CERTIFICATE REQUEST" on page 1383	Global Configuration	Creates certificate enrollment requests for submittal to public or private CAs.
"SERVICE HTTPS" on page 1385	Global Configuration	Enables the HTTPS web server.
"IP HTTPS CERTIFICATE" on page 1386	Global Configuration	Designates the active certificate of the HTTPS web server.
"NO SERVICE HTTPS" on page 1387	Global Configuration	Disables the HTTPS web browser server.
"SHOW CRYPTO CERTIFICATE" on page 1388	Privileged Exec	Displays detailed information about the certificates on the switch.
"SHOW IP HTTPS" on page 1389	Privileged Exec	Displays the settings of the HTTPS web browser server.

CRYPTO CERTIFICATE DESTROY

Syntax

```
crypto certificate id_number destroy
```

Parameters

id_number
> Specifies the ID number of a certificate to be deleted from the switch. The range is 0 to 10. You can enter just one ID number.

Mode

Global Configuration mode

Description

Use this command to delete unused certificates from the switch. You can delete just one certificate at a time with this command.

Entering the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command after deleting a certificate is unnecessary because certificates are not stored in the active boot configuration file.

Confirmation Command

"SHOW IP HTTPS" on page 1389

Example

This example deletes the certificate with the ID number 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto certificate 5 destroy
```

CRYPTO CERTIFICATE GENERATE

Syntax

```
crypto certificate id_number generate length passphrase
common_name organizational_unit organization location state
country duration
```

Parameters

id_number

> Specifies a certificate ID number. The range is 0 to 10. A certificate must be assigned an ID number that is unique from the ID numbers of all other certificates already on the switch.

length

> Specifies the length of the encryption key in bits. The range is 512 to 1536 bits. The default is 512 bits.

passphrase

> Specifies a passphrase, used to export the certificate in PKCS12 file format. This parameter must be from 4 to 20 characters. Spaces and special characters are not allowed. (Even though the switch does not permit the export of certificates, a passphrase is still required in the command.)

common_name

> Specifies a common name for the certificate. This should be the IP address or fully qualified URL designation of the switch. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

organizational_unit

> Specifies the name of a department, such as Network Support or IT. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

organization

> Specifies the name of a company. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

location

> Specifies a location of the switch. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

state

> Specifies a state, such as California or Nevada. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

country

Specifies the ISO 3166-1 initials of a country. This parameter must be two uppercase characters.

duration

Specifies the number of days the certificate is valid. The range is 30 to 3650 days.

Note
For a valid certificate to be active, you need to set the system clock. See "Manually Setting the Date and Time" on page 117 or "Activating the SNTP Client and Specifying the IP Address of an NTP or SNTP Server" on page 325.

Mode

Global Configuration mode

Description

Use this command to create self-signed certificates for secure HTTPS web browser management of the switch. All the parameters in the command are required.

Entering the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command after creating a self-signed certificate is unnecessary because certificates are not stored in the active boot configuration file.

Note
Generating a certificate is CPU intensive. It should be performed before the switch is connected to your network or during periods of low network activity.

Confirmation Command

"SHOW IP HTTPS" on page 1389

Example

This example creates a self-signed certificate with the following specifications:

- ❒ ID number: 2
- ❒ Key length: 1280
- ❒ Passphrase: trailtree
- ❒ Common name: 167.214.121.45

- ❒ Organizational unit: Sales

- ❒ Organization: Jones_Industries

- ❒ Location: San_Jose

- ❒ State: California

- ❒ Country: US

- ❒ Duration: 365 days

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto certificate 2 generate 1280 trailtree
167.214.121.45 Sales Jones_Industries San_Jose California US
365
```

CRYPTO CERTIFICATE IMPORT

Syntax

```
crypto certificate id_number import
```

Parameters

id_number
Specifies the ID number of a certificate to be imported into the certificate database on the switch. You can specify just one ID number.

Mode

Global Configuration mode

Description

Use this command to import certificates from public or private CAs into the certificate database of the switch. A certificate has to be residing in the file system on the switch before you can import it into the certificate database.

Entering the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command after importing a certificate is unnecessary because certificates are not stored in the active boot configuration file.

Confirmation Command

"SHOW IP HTTPS" on page 1389

Example

This example imports a certificate with the ID number 2 into the certification database from the file system:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto certificate 2 import
```

CRYPTO CERTIFICATE REQUEST

Syntax

```
crypto certificate id_number request common_name
organizational_unit organization location state country
```

Parameters

id_number

Specifies a certificate ID number. The range is 0 to 10. A certificate must be assigned an ID number that is unique from the ID numbers of any certificates already on the switch.

common_name

Specifies a common name for the certificate. This should be the IP address or fully qualified URL designation of the switch. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

organizational_unit

Specifies the name of a department, such as Network Support or IT. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

organization

Specifies the name of a company. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

location

Specifies the location of the switch. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

state

Specifies the state, such as California or Nevada. This parameter can have up to 64 characters. Spaces and special characters are not allowed.

country

Specifies the ISO 3166-1 initials of the country. This parameter must be two uppercase characters.

Mode

Global Configuration mode

Description

Use this command to create certificate enrollment requests for submittal to public or private CAs. Enrollment requests are stored in the file system in Base64-encoded X.509 format, with a ".pem" extension.

Note

An enrollment request must have the same ID number and other information as its corresponding self-signed certificate.

Confirmation Command

"DIR" on page 467

Example

This example creates a certificate enrollment request that has these specifications:

- ❐ ID number: 2
- ❐ Common name: 167.214.121.45
- ❐ Organizational unit: Sales
- ❐ Organization: Jones_Industries
- ❐ Location: San_Jose
- ❐ State: California
- ❐ Country: US

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto certificate 2 request 167.214.121.45
Sales Jones_Industries San_Jose California US
```

SERVICE HTTPS

Syntax

```
service https
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to activate the HTTPS web server on the switch. The switch supports secure HTTPS web browser management sessions when the server is activated. Here are the preconditions to activating the server:

❐ The non-secure HTTP server on the switch must be disabled. For instructions, refer to "NO SERVICE HTTP" on page 1360.

❐ The switch must have an HTTPS certificate that was designated as the active certificate with the IP HTTPS CERTIFICATE command.

Confirmation Command

"SHOW IP HTTPS" on page 1389

Example

This example activates the HTTPS web server on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# service https
```

IP HTTPS CERTIFICATE

Syntax

```
ip https certificate id_number
```

Parameters

id_number

 Specifies a certificate ID number.

Mode

Global Configuration mode

Description

Use this command to designate the active certificate for the secure HTTPS web server. The switch can have only one active certificate. The certificate, which must already exist on the switch, can be a self-signed certificate that the switch created itself or a certificate that was issued by a CA, from a certificate request generated by the switch.

Confirmation Command

"SHOW IP HTTPS" on page 1389

Example

This example designates the certificate with the ID number 1 as the active certificate on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip https certificate 1
```

NO SERVICE HTTPS

Syntax

```
no service https
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the secure HTTPS web server on the switch. The switch rejects secure HTTPS web browser management sessions when the server is deactivated. You might disable the server to prevent remote web browser management sessions of the switch or prior to activating the non-secure HTTP web browser server.

Confirmation Command

"SHOW IP HTTPS" on page 1389

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no service https
```

SHOW CRYPTO CERTIFICATE

Syntax

```
show crypto certificate id_number
```

Parameters

id_number
        Specifies a certificate ID number.

Mode

Privileged Exec mode

Description

Use this command to display detailed information about the certificates on the switch. You can display just one certificate at a time.

Example

This example displays detailed information about the certificates on the switch:

```
awplus# show crypto certificate 1
```

SHOW IP HTTPS

Syntax

```
show ip http
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the status of the HTTPS server and basic information about the certificates on the switch. An example of the information is shown here.

```
HTTPS server enabled. Port: 443
Certificate 1 is active
Issued by: self-signed
Valid from: 5/17/2010 to 5/16/2011
Subject: C=US, ST=California, L=San_Jose, O=Jones_Industries, OU=Sales,
CN=167.214.121.45
Finger print: 3FB9D543 72D8E6F8 2159F35E B634A738
```

Figure 218. SHOW IP HTTPS Command

The fields are defined in Table 153.

Table 153. SHOW IP HTTPS Command

Field	Description
HTTPS server enabled	Indicates that the HTTPS server is activated on the switch. This line is not displayed when the server is disabled.
Port	The TCP port number of the server. This parameter, which cannot be changed, is not displayed when the server is disabled.

Table 153. SHOW IP HTTPS Command (Continued)

Field	Description
Certificate # is active|inactive	Displays the status of the certificate. An active status indicates that the certificate was designated with "IP HTTPS CERTIFICATE" on page 1386 as the active certificate for the HTTPS server. The switch can have just one active certificate.
Valid from	Displays the dates during which the certificate is valid.
Subject	Displays certificate configuration information.

Example

This example displays the status of the HTTPS server and basic information about the certificates on the switch:

```
awplus# show ip https
```

Chapter 88

RADIUS and TACACS+ Clients

This chapter describes the following topics:

Overview

The switch has RADIUS and TACACS+ clients for remote authentication. Here are the two features that use remote authentication:

❒ 802.1x port-based network access control. This feature lets you increase network security by requiring that network users log on with user names and passwords before the switch will forward their packets. This feature is described in Chapter 60, "802.1x Port-based Network Access Control" on page 893.

❒ Remote manager accounts. This feature lets you add more manager accounts to the switch by transferring the task of authenticating the accounts from the switch to an authentication server on your network. This feature is described in "Remote Manager Accounts" on page 1393.

The RADIUS client supports both features, but the TACACS+ client supports only the remote manager accounts feature. Here are the guidelines:

❒ Only one client can be active on the switch at a time.

❒ If you want to use just the remote manager account feature, you can use either RADIUS or TACACS+ because both clients support that feature.

❒ If you want to use 802.1x port-based network access control, you have to use the RADIUS client because the TACACS+ client does not support that feature.

Remote Manager Accounts

The switch has one local manager account. The account is referred to as a local account because the switch authenticates the user name and password when a manager uses the account to log on. If the user name and password are valid, the switch allows the individual to access its management software. Otherwise, it cancels the login to prevent unauthorized access.

There are two ways to add more manager accounts. One way is to create additional local accounts. This is explained in Chapter 76, "Local Manager Accounts" on page 1289 and Chapter 77, "Local Manager Account Commands" on page 1301. There can be up to eight local manager accounts.

The other way to add more accounts is with a RADIUS or TACACS+ authentication server on your network. With these features, the authentication of the user names and passwords of the manager accounts is performed by one or more authentication servers. The switch forwards the information to the servers when managers log on. The following steps illustrate the authentication process that occurs between the switch and an authentication server when a manager logs on:

1. The switch uses its RADIUS or TACACS+ client to transmit the user name and password to an authentication server on the network.

2. The server checks to see if the user name and password are valid.

3. If the combination is valid, the authentication server notifies the switch, which completes the login process, allowing the manager access to its management software.

4. If the user name and password are invalid, the authentication protocol server notifies the switch, which cancels the login.

As explained in "Privilege Levels" on page 1290, local manager accounts can have a privilege level of 1 or 15. Managers with a privilege level of 15 have access to all command modes. Managers with accounts that have a privilege level of 1 are restricted to the User Exec mode when command mode restriction is active on the switch, unless they know the special password.

Privilege levels also apply to remote manager accounts. When you create accounts on an authentication server, assign them a level of 1 or 15, just like local accounts. If command mode restriction is active on the switch, managers with a privilege level of 1 are limited to the User Exec mode, while managers with a privilege level of 15 are given access to the entire command mode structure. If command mode restriction is not active on

1393

the switch, the privilege level of an account is ignored and all accounts have access to the entire command mode structure.

Here are the main steps to using the remote manager accounts feature on the switch:

1. Install TACACS+ or RADIUS server software on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesis.

2. Add the new manager accounts to the authentication servers. Here are the guidelines:

    – Assign each account a user name and password. The maximum length of a user name is 38 alphanumeric characters and spaces, and the maximum length of a password is 16 alphanumeric characters and spaces.

    – Assign each account a privilege level. This process differs depending on the server software. The TACACS+ server provides sixteen levels of the Privilege attribute (0 to 15); however, the AT-9000 switch provides only two settings of the Privilege attribute (0 or 15). If command mode restriction is active on the switch, a manager account with a privilege level of 0 is restricted to the User Exec mode, while an account with a privilege level of 15 has access to all the command modes.

    Note
    If you enter a value other than 0 or 15 for the TACACS+ privilege level, the switch does not recognize the privilege level and responds with a "failed to authenticate" error message.

    For RADIUS, the management level is controlled by the Service Type attribute. Of its 11 values, only two apply to the switch. A value of "NAS Prompt" is equivalent to a privilege level of 1, while a value of "Administrative" is equivalent to the privilege level 15.

    Note
    This manual does not explain how to configure a TACACS+ or RADIUS server. For instructions, refer to the documentation included with the server software.

3. Assign the switch a management IP address. For instructions, refer to "What to Configure First" on page 70 or Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

4. Configure the RADIUS or TACACS+ client on the switch by entering the IP addresses of up to three authentication servers. For instructions, refer to "Managing the RADIUS Client" on page 1396 or "Managing the TACACS+ Client" on page 1400.

5. Enable the TACACS+ or RADIUS client.

6. Activate remote manager authentication on the switch. For instructions, refer to "Configuring Remote Authentication of Manager Accounts" on page 1403.

> **Note**
> For information on the RADIUS and TACACS+ authentication protocols, refer to the RFC 2865 and RFC 1492 standards, respectively.

Guidelines

Here are the guidelines to using the RADIUS and TACACS+ clients:

❒ Only one client can be active on the switch at a time.

❒ The clients can have a maximum of three IP addresses of authentication servers.

❒ The switch must have a management IP address. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The authentication servers on your network must be members of the same subnet as the management IP address of the switch or have access to it through routers or other Layer 3 devices.

❒ If the authentication servers are not members of the same subnet as the management IP address, the switch must have a default gateway. The default gateway defines the IP address of the first hop to reaching the remote subnet of the servers. For instructions, refer to Chapter 13, "IPv4 and IPv6 Management Addresses" on page 285.

❒ The client polls the servers for authentication information in the order in which they are listed in the client.

❒ The switch does not support the two earlier versions of the TACACS+ protocol, TACACS and XTACACS.

❒ The TACACS+ client does not support 802.1x port-based network access control. You must use the RADIUS client and a RADIUS server for that feature.

Managing the RADIUS Client

The following subsections describe how to manage the RADIUS client:

❒ "Adding IP Addresses of RADIUS Servers" next

❒ "Specifying a RADIUS Global Encryption Key" on page 1397

❒ "Specifying the Server Timeout" on page 1397

❒ "Specifying RADIUS Accounting" on page 1398

❒ "Removing the Accounting Method List" on page 1398

❒ "Deleting Server IP Addresses" on page 1399

❒ "Displaying the RADIUS Client" on page 1399

Adding IP Addresses of RADIUS Servers

The RADIUS client can store up to three IP addresses of RADIUS servers on your network. The order that you add an IP address determines its order on the switch. For instance, the first IP address that you add becomes server one, the second IP address that you add becomes server two, and the third IP address that you add becomes server three. Also, when you remove an IP address from the switch, the IP addresses below it are moved up. For example, if you make the following assignments:

❒ server one is 186.178.11.154

❒ server two is 186.178.11.156

❒ server three is 186.178.11.158

If you delete server one with an IP address of 186.178.11.154, server two remains the IP address of 186.178.11.156 and moves up to server one in the list, and the IP address of 186.178.11.158 moves up to server two. As a result, the next server address that you add to the switch is added to the bottom of the list and becomes server three.

To add an IP address, use the RADIUS-SERVER HOST command in the Global Configuration mode. Here is the format of the command:

```
radius-server host ipaddress [acct-port value] [auth-port
value] [key value]
```

You can add only one address at a time with this command.

The HOST parameter specifies the IP address of a RADIUS server on the network.

The ACCT-PORT parameter specifies the accounting port. This is 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.

The AUTH-PORT parameter 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.

The KEY parameter specifies the encryption key used by the designated RADIUS server. The maximum length is 40 characters.

The AUTH-PORT parameter specifies the UDP destination port for RADIUS authentication requests. The default UDP port is 1812.

The KEY parameter specifies the encryption key used by the designated RADIUS server. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

This example adds the IP address 111.111.111.111 as the second address in the list. The accounting port is 1811, and the authentication port is 1815. The encryption key is "ATI:"

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server host 111.111.111.111 acct-port
1811 auth-port 1815 key ATI
```

Specifying a RADIUS Global Encryption Key

If the RADIUS servers on your network use the same encryption key, use the RADIUS-SERVER KEY command in the Global Configuration mode to enter a global encryption key in the client. The format of the command is:

```
radius-server key secret
```

This example specifies "4tea23" as the global encryption key of the RADIUS servers:

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server key 4tea23
```

To remove the global encryption key without specifying a new value, use the NO form of this command:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server key
```

Specifying the Server Timeout

When the switch sends an authentication request to a RADIUS server, it waits a predefined time period for a response. This time period is referred to as the server timeout value. If the switch does not receive a response to an authentication request, it queries the next server in the list. If none of the servers respond, the switch activates the local manager accounts.

To set the server timeout period, use the RADIUS-SERVER TIMEOUT command in the Global Configuration mode. The range is 1 to 1000 seconds. The default is 5 seconds.

This example sets the RADIUS timeout to 15 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server timeout 15
```

Specifying RADIUS Accounting

To specify RADIUS accounting for *all* shell login sessions, use the AAA ACCOUNTING LOGIN command in the Global Configuration mode. Here is the format of the command:

```
aaa accounting login default start-stop|stop-only|none group
radius|tacacs [local]
```

The DEFAULT parameter indicates the default accounting method list.

The START-STOP parameter indicates a start accounting message is sent at the beginning of a session, and a stop accounting message is sent at the end of the session.

The STOP-ONLY parameter indicates a stop accounting message is sent at the end of the session.

The NONE parameter disables accounting messages.

The GROUP parameter indicates the user server group. Specify the RADIUS server.

The LOCAL parameter indicates that if the first attempt to authenticate a user with the RADIUS server fails, the authentication process fails, and the user is approved to access the switch with the local name and password.

This example configures RADIUS accounting for all login shell sessions to send a start accounting message at the beginning of a session and a stop accounting message at the end of the session:

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

Removing the Accounting Method List

To reset the configuration of the default accounting list for login shell sessions, use the NO AAA ACCOUNTING LOGIN DEFAULT command. This command causes the switch to revert to the authentication method used by the local user database:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa accounting login default
```

Deleting Server IP Addresses

To delete the IP address of a RADIUS server from the list of servers on the switch, use the NO RADIUS-SERVER HOST command in the Global Configuration mode. You can delete only one IP address at a time with this command. This example removes the IP address 211.132.123.12 from the list of RADIUS servers:
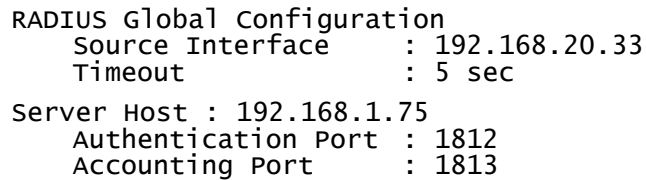
```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server host 211.132.123.12
```

Displaying the RADIUS Client

To display the settings of the RADIUS client, use the SHOW RADIUS command in the User Exec mode or Privileged Exec mode.

```
awplus# show radius
```

Here is an example of the RADIUS client information.

```
RADIUS Global Configuration
    Source Interface    : 192.168.20.33
    Timeout             : 5 sec
Server Host : 192.168.1.75
    Authentication Port : 1812
    Accounting Port     : 1813
```

Figure 219. SHOW RADIUS Command

The information is described in Table 155 on page 1426.

Managing the TACACS+ Client

The following subsections describe how to manage the TACACS+ client:

❒ "Adding IP Addresses of TACACS+ Servers" next

❒ "Specifying TACACS+ Accounting" on page 1401

❒ "Deleting IP Addresses of TACACS+ Servers" on page 1402

❒ "Removing the Accounting Method List" on page 1401

❒ "Displaying the TACACS+ Client" on page 1402

Adding IP Addresses of TACACS+ Servers

The TACACS+ client can store the IP addresses of three TACACS+ servers on your network. The order that you add an IP address determines its order on the switch. For instance, the first IP address that you add becomes server one, the second IP address that you add becomes server two, and the third IP address that you add becomes server three. Also, when you remove an IP address from the switch, the IP addresses below it are moved up. For example, if you make the following assignments:

❒ server one is 186.178.11.154

❒ server two is 186.178.11.156

❒ server three is 186.178.11.158

If you delete the IP address of 186.178.11.154 for server one in the list, the server two IP address of 186.178.11.156 moves up to the server one position, and the IP address of 186.178.11.158 moves up to the server two position. As a result, the next server address that you add to the switch is added to the bottom of the list and becomes server three.

Use the TACACS-SERVER HOST command in the Global Configuration mode command to add an IP address of a server to the client. Here is the format of the command:

```
tacacs-server host ipaddress key value
```

You can add only one IP address at a time with this command.

The HOST parameter specifies an IP address of a TACACS+ server.

The KEY parameter specifies the secret key of a TACACS+ server. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

pg 1401

This example adds the IP address 115.16.172.54 as a TACACS+ authentication server at the bottom of the list. The server has the key "prt17:"

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server host 115.16.172.54 key prt17
```

Specifying TACACS+ Accounting

To specify TACACS+ accounting for *all* shell login sessions, use the AAA ACCOUNTING LOGIN command in the Global Configuration mode. Here is the format of the command:

```
aaa accounting login default start-stop|stop-only|none group
radius|tacacs
```

The DEFAULT parameter indicates the default accounting method list.

The START-STOP parameter indicates a start accounting message is sent at the beginning of a session, and a stop accounting message is sent at the end of the session.

The STOP-ONLY parameter indicates a stop accounting message is sent at the end of the session.

The NONE parameter disables accounting messages.

The GROUP parameter indicates the user server group. Specify the TACACS+ server.

This example configures TACACS+ accounting for all login shell sessions to send a start accounting message at the beginning of a session and a stop accounting message at the end of the session:

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

Removing the Accounting Method List

To reset the configuration of the default accounting list for login shell sessions, use the NO AAA ACCOUNTING LOGIN DEFAULT command. This command causes the switch to revert to the authentication method used by the local user database:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa accounting login default
```

Deleting IP Addresses of TACACS+ Servers

To delete the IP address of a TACACS+ server from the client on the switch, use the NO TACACS-SERVER HOST command in the Global Configuration mode. You can delete only one IP address at a time with this command. This example removes the IP address 122.124.15.7 from the TACACS+ client:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server host 122.114.15.7
```

Displaying the TACACS+ Client

To display the settings of the TACACS+ client, use the SHOW TACACS command in the Privileged Exec mode.

```
awplus# show tacacs
```

Here is an example of the TACACS+ client information.

```
TACACS+ Global Configuration
   Timeout              : 5 sec

Server Host/    Server
IP Address      Status
----------------------
10.0.0.170      Alive
192.168.1.166   Unknown
```

Figure 220. SHOW TACACS Command

The fields are explained in Table 156 on page 1428.

Configuring Remote Authentication of Manager Accounts

Check that you performed the following steps before activating remote authentication of manager accounts on the switch:

❒ Added at least one RADIUS or TACACS+ server to your network.

❒ Added the manager accounts to the authentication servers.

❒ Assigned a management IP address to the switch.

❒ Added the IP addresses of the authentication servers to the RADIUS or TACACS+ client on the switch.

To activate the feature, use the AAA AUTHENTICATION LOGIN commands in the Global Configuration mode. The commands for the two clients are different. If you are using RADIUS, enter:

```
awplus> enable
awplus# configure terminal
awplus(config)# aaa authentication login radius
```

If you are using TACACS+, enter:

```
awplus> enable
awplus# configure terminal
awplus(config)# aaa authentication login tacacs
```

After you activate the feature, all future login attempts by managers are forwarded by the switch to the designated authentication servers for authentication.

To deactivate the feature, use the NO versions of the commands. The following example deactivates the feature if it is using RADIUS:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa authentication login radius
```

The following example deactivates the feature if it is using TACACS+:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa authentication login tacacs
```

The switch supports both local and remote manager accounts at the same time for different management methods. You can toggle the remote manager authenticator on or off for local, Telnet, and SSH management sessions. For example, you may configure the switch to use its local manager accounts for local management sessions and remote manager accounts for Telnet and SSH management sessions. You can even toggle remote authentication on or off for the ten individual VTY lines the switch

uses for remote Telnet and SSH sessions. (For background information, refer to "VTY Lines" on page 69.)

Toggling remote authentication is accomplished with the LOGIN AUTHENTICATION and NO LOGIN AUTHENTICATION commands, found in the Console Line and Virtual Terminal Line modes. Here are several examples of how to use the commands.

Assume you used the appropriate AAA AUTHENTICATION LOGIN command to activate remote authentication on the switch. At the default settings, the switch activates remote authentication for all local, Telnet, and SSH management sessions. Now assume that you want the switch to use the local manager accounts instead of the remote manager accounts whenever anyone logs in using the Console port. To do this, you need to toggle off remote authentication for local management sessions using the NO LOGIN AUTHENTICATION command in the Console Line mode, as shown here:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no login authentication
```

Now, even though remote authentication is activated, the switch uses its local manager accounts to authenticate the user name and password whenever someone logs on through the Console port.

If you change your mind and want to reactivate remote authentication for local management sessions, enter the LOGIN AUTHENTICATION command, again in the Console Line mode, as shown here:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# login authentication
```

Toggling remote authentication for Telnet and SSH management sessions is more complex because there are ten VTY lines and you can toggle remote authentication on each line individually. For example, you might configure the lines so that the switch uses its local manager accounts to authenticate management sessions on lines 0 and 1, and the remote manager accounts on the other lines.

Toggling remote authentication on the VTY lines is performed with the same commands as for local management sessions, but in different modes. They are called VTY Line modes, and there is one mode for each line. The command for entering the modes is the LINE VTY command, which has this format:

```
line vty line_id
```

1404

The LINE_ID parameter has a range of 0 to 9. The following example of the command toggles off remote authentication on VTY line 0.

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0
awplus(config-line)# no login authentication
```

Now, the switch uses the local manager accounts, instead of the remote accounts, to authenticate the user name and password when an administrator establishes a Telnet or SSH management session on VTY line 0.

The following example reactivates remote authentication on VTY line 0:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0
awplus(config-line)# login authentication
```

Chapter 89

RADIUS and TACACS+ Client Commands

The commands for the RADIUS and TACACS+ clients are summarized in Table 154 and described in detail within the chapter.

Table 154. RADIUS and TACACS+ Client Commands

Command	Mode	Description
"AAA ACCOUNTING LOGIN" on page 1409	Global Configuration	Configures RADIUS or TACACS+ accounting for login shell session.
"AAA AUTHENTICATION ENABLE (TACACS+)" on page 1411	Global Configuration	Enables the TACACS+ password on the switch.
"AAA AUTHENTICATION LOGIN" on page 1413	Global Configuration	Enables RADIUS or TACACS+ on the switch globally.
"IP RADIUS SOURCE-INTERFACE" on page 1415	Global Configuration	Configures the RADIUS source IP address interface.
"LOGIN AUTHENTICATION" on page 1417	Console Line and Virtual Terminal Line	Activates remote authentication for local management sessions and remote Telnet and SSH sessions.
"NO LOGIN AUTHENTICATION" on page 1419	Console Line and Virtual Terminal Line	Deactivates remote authentication for local management sessions and remote Telnet and SSH sessions.
"NO RADIUS-SERVER HOST" on page 1420	Global Configuration	Deletes IP addresses of RADIUS servers from the list of authentication servers in the RADIUS client.
"NO TACACS-SERVER HOST" on page 1421	Global Configuration	Deletes IP addresses of TACACS+ servers from the list of authentication servers in the TACACS+ client.
"RADIUS-SERVER HOST" on page 1422	Global Configuration	Adds IP addresses of RADIUS servers to the RADIUS client for remote authentication and accounting.
"RADIUS-SERVER KEY" on page 1424	Global Configuration	Specifies the global encryption key of the RADIUS servers.

1407

Table 154. RADIUS and TACACS+ Client Commands (Continued)

Command	Mode	Description
"RADIUS-SERVER TIMEOUT" on page 1425	Global Configuration	Specifies the maximum amount of time the RADIUS client waits for a response from a RADIUS authentication server for an authentication request.
"SHOW RADIUS" on page 1426	Privileged Exec	Displays the configuration settings of the RADIUS client.
"SHOW TACACS" on page 1428	Privileged Exec	Displays the configuration settings of the TACACS+ client.
"TACACS-SERVER HOST" on page 1430	Global Configuration	Adds IP addresses of TACACS+ servers to the TACACS+ client in the switch.
"TACACS-SERVER KEY" on page 1431	Global Configuration	Specifies the global encryption key of the TACACS+ servers.
"TACACS-SERVER TIMEOUT" on page 1432	Global Configuration	Specifies the maximum amount of time the TACACS+ client waits for a response from a TACACS+ authentication server for an authentication request.

AAA ACCOUNTING LOGIN

Syntax

aaa accounting login *default start-stop|stop-only|none group radius|tacacs*

Parameters

default

    Indicates the default accounting method list.

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 the session.

none

    Disables accounting messages.

group

    Indicates the user server group. Specify one of the following:

        radius: Uses all RADIUS servers.

        tacacs: Uses all TACACS+ servers.

Mode

Global Configuration mode

Description

This command configures RADIUS or TACACS+ accounting for all login shell sessions. This command creates a default method list that is applied to every console and vty line unless another accounting method list is applied on that line.

Use the no form of this command, NO AAA ACCOUNTING LOGIN DEFAULT, to remove the accounting method list for login shell sessions. This command causes the switch to revert to the authentication method used by the local user database. In addition, it disables accounting on every line that has the default accounting configuration.

1409

Confirmation Commands

"SHOW RADIUS" on page 1426

"SHOW TACACS" on page 1428

Examples

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

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

To reset the configuration of the default accounting list, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# no aaa accounting login default
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

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

AAA AUTHENTICATION ENABLE (TACACS+)

Syntax

```
aaa authentication enable default group tacacs [local]
```

Parameters

default
> Indicates the default accounting method list.

group
> Indicates the user server group. Specify the following:
>
> > *tacacs:* Uses all TACACS+ servers.

local
> Indicates that authentication using the password provided in the ENABLE PASSWORD command is attempted if a TACACS+ server is not available. For information about this command, see "ENABLE PASSWORD" on page 1302. This is an optional parameter.

Mode

Global Configuration mode

Description

Use this command to enable the TACACS+ password on the switch. This password is used to verify the TACACS+ server, thereby providing another layer of security. By default, the AAA AUTHENTICATION ENABLE command is disabled.

> **Note**
> This command only applies to TACACS+ clients.

Use the no form of this command, NO AAA AUTHENTICATION ENABLE, to disable the TACACS+ password on the switch.

Confirmation Commands

"SHOW TACACS" on page 1428

Examples

To enable the TACACS+ password on the switch and specify authentication using the password provided in the ENABLE PASSWORD

1411

command is attempted if a TACACS+ server is not available, use the following commands:

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

To enable the TACACS+ password on the switch, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# aaa authentication enable default group
tacacs
```

1412

AAA AUTHENTICATION LOGIN

Syntax

```
aaa authentication login default [group radius|tacacs]
[local]
```

Parameters

default

Indicates the default accounting method list.

group

Indicates the user server group. Specify one of the following:

radius: Uses all RADIUS servers.

tacacs: Uses all TACACS+ servers.

local

Indicates that authentication using the password provided in the ENABLE PASSWORD command is attempted if a RADIUS or TACACS+ server is not available. For information about this command, see "ENABLE PASSWORD" on page 1302. This is an optional parameter.

Mode

Global Configuration mode

Description

Use this command to enable RADIUS or TACACS+ on the switch globally. This command creates an ordered list of methods used to authenticate a RADIUS or TACACS+ user login. Specify the local parameter or the group parameter in the order that you want these parameters to be applied.

Use the no version of this command, NO AAA AUTHENTICATION LOGIN, to remove the authentication setting on the switch. This command returns the default method list to its default state which is local.

> **Note**
> The NO AAA AUTHENTICATION LOGIN command does not remove the default method list from the software.

Confirmation Commands

"SHOW RADIUS" on page 1426

"SHOW TACACS" on page 1428

Examples

To enable RADIUS servers on the switch, use the following commands:

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

To enable TACACS+ servers on the switch, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# aaa authentication login default group
tacacs local
```

1414

IP RADIUS SOURCE-INTERFACE

Syntax

```
ip radius source-interface Ipv4 Address | VID
```

Parameters

Ipv4 Address
    Indicates an IPv4 address in the following format:

    xxx.xxx.xxx.xxx

VID
    Specifies a VLAN ID.

Modes

Global Configuration mode

Description

Use this command to assign the RADIUS source interface to an IPv4 address or VLAN ID. The RADIUS client uses the specified IP address on every outgoing RADIUS packet.

Use the no version of this command, NO IP RADIUS SOURCE-INTERFACE, to remove the RADIUS source IP address from the client.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example configures the RADIUS source IP address using a VLAN ID:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip radius source-interface vlan 1
```

This example configures the RADIUS source IP address with an IPv4 address:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.78
```

This example removes the RADIUS source IP address from the RADIUS client:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

LOGIN AUTHENTICATION

Syntax

```
login authentication
```

Parameters

None

Modes

Console Line and Virtual Terminal Line modes

Description

Use this command to activate remote authentication of manager accounts for local management sessions and remote Telnet and SSH sessions.

You can activate remote authentication separately for the different management methods. Remote authentication of local management sessions is activated in the Console Line mode while remote authentication for remote Telnet and SSH management sessions is activated in the Virtual Terminal Line mode.

> **Note**
> If the switch is unable to communicate with the authentication servers when a manager logs on, because either the servers are not responding or the RADIUS or TACACS+ client is configured incorrectly, the switch automatically reactivates the local manager accounts so that you can continue to log on and manage the unit.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example activates remote authentication for local management sessions:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# login authentication
```

This example activates remote authentication for remote Telnet and SSH management sessions that use VTY line 0:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0
awplus(config-line)# login authentication
```

1418

NO LOGIN AUTHENTICATION

Syntax

```
no login authentication
```

Parameters

None

Modes

Console Line and Virtual Terminal Line modes

Description

Use this command to deactivate remote authentication for local management sessions and remote Telnet and SSH sessions.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 158

Examples

This example deactivates remote authentication for local management sessions:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no login authentication
```

This example deactivates remote authentication on VTY line 0, used by remote Telnet and SSH management sessions:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0
awplus(config-line)# no login authentication
```

NO RADIUS-SERVER HOST

Syntax

```
no radius-server host ipaddress
```

Parameter

ipaddress
    Specifies an IP address of a RADIUS server to be deleted from the authentication server list.

Mode

Global Configuration mode

Description

Use this command to delete IP addresses of RADIUS servers from the list of authentication servers on the switch. You can delete only one IP address at a time with this command.

Confirmation Command

"SHOW RADIUS" on page 1426

Example

This example removes the IP address 122.34.122.47 from the list of RADIUS servers:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server host 122.34.122.47
```

NO TACACS-SERVER HOST

Syntax

```
no tacacs-server host ipaddress
```

Parameter

ipaddress

Specifies an IP address of a TACACS+ server to be deleted from the TACACS+ client. You can delete just one address at a time with this command.

Mode

Global Configuration mode

Description

Use this command to delete IP addresses of TACACS+ servers from the client. You can delete only one IP address at a time with this command.

Confirmation Command

"SHOW TACACS" on page 1428

Example

This example removes the IP address 152.112.12.7 from the TACACS+ client:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server host 152.112.12.7
```

RADIUS-SERVER HOST

Syntax

radius-server host *ipaddress* [acct-port *value*] [auth-port *value*] [key *value*]

Parameters

ipaddress

Specifies the IP address of a RADIUS server on the network.

acct-port

Specifies the accounting port. This is 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.

auth-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.

key

Specifies the encryption key used by the designated RADIUS server. The maximum length is 40 characters.

Mode

Global Configuration mode

Description

Use this command to add IP addresses of RADIUS servers to the authentication server list on the switch. Servers defined with this command are used for remote authentication only.

The switch can have up to three RADIUS authentication servers, but only one can be added at a time with this command. The order that you add an IP address determines its order on the switch.

Confirmation Command

"SHOW RADIUS" on page 1426

1422

Examples

This example adds a RADIUS server with the IP address 176.225.15.23. The UDP port is 1811, and the encryption key is "abt54:"

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server host 176.225.15.23 auth-port
1811 key abt54
```

This example adds the IP address 149.245.22.22 of a RADIUS server to the RADIUS client on the switch. The UDP port is 1815, and the encryption key is "tiger12:"

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server host 149.245.22.22 auth-port
1815 key tiger12
```

This example adds a RADIUS server with the IP address 176.225.15.23 to the switch. The accounting port is 1811, and the UDP port is 1815. The encryption key is "kieran7:"

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server host 176.225.15.23 acct-port
1811 auth-port 1815 key kieran7
```

This example adds the IP address 149.245.22.22 of a RADIUS server to the RADIUS client on the switch. The accounting port is set to 0 which indicates the server is not used for accounting. The UDP port is 1814, and the encryption key is "jared6:"

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server host 149.245.22.22 acct-port 0
auth-port 1814 key jared6
```

RADIUS-SERVER KEY

Syntax

```
radius-server key value
```

Parameters

key

   Specifies the global encryption key of the RADIUS servers. The maximum length is 40 characters.

Mode

Global Configuration mode

Description

Use this command to add the global encryption key of the RADIUS servers to the RADIUS client. You can add a global encryption key if you defined one RADIUS server in the RADIUS client; or if there is more than one server, and they all use the same encryption key. To define two or three servers that use different encryption keys, do not enter a global encryption key with this command. Instead, define the individual keys when you add the IP addresses of the servers to the client with "RADIUS-SERVER HOST" on page 1422.

To remove an existing global key without specifying a new value, use the NO form of this command, NO RADIUS-SERVER KEY.

Confirmation Command

"SHOW RADIUS" on page 1426

Examples

This example sets the RADIUS global encryption key to 'key22a':

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server key key22a
```

This example deletes the current RADIUS global encryption key without defining a new value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server key
```

RADIUS-SERVER TIMEOUT

Syntax

```
radius-server timeout value
```

Parameters

timeout
>   Specifies the maximum amount of time the RADIUS client waits for a response from a RADIUS authentication server. The range is 1 to 1,000 seconds. The default is 5 seconds.

Mode

Global Configuration mode

Description

Use this command to set the timeout value for the RADIUS client on the switch. The timeout is the amount of time the client waits for a response from a RADIUS server for an authentication request. If the timeout expires without a response, the client queries the next server in the list. If there are no further servers in the list to query, the switch defaults to the standard manager and operator accounts.

Use the no form of this command, NO RADIUS-SERVER TIMEOUT, to set the RADIUS timeout to the default value of 5 seconds.

Confirmation Command

"SHOW RADIUS" on page 1426

Examples

This example sets the RADIUS timeout to 55 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server timeout 55
```

This example returns the RADIUS timeout to the default value of 5 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server timeout
```

SHOW RADIUS

Syntax

show radius

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the configuration of the RADIUS client. Here is an example of the client information.

```
RADIUS Global Configuration
    Source Interface    : 192.168.3.97
    Timeout             : 5 sec
 Server Host : 192.168.1.75
    Authentication Port : 1812
    Accounting Port     : 1813
```

Figure 221. SHOW RADIUS Command

The fields are defined in this table.

Table 155. SHOW RADIUS Command

Parameter	Description
Source Interface	An IP address assigned to an interface on the switch that is the source of all outgoing RADIUS packets. WIth hardware stacking, this the source address of the master switch.
Timeout	The length of the time, in seconds, that the switch waits for a response from a RADIUS server to an authentication request, before querying the next server in the list.
Server Host	The IP address of a RADIUS server on the network.
Authentication Port	The authentication protocol port.

1426

Table 155. SHOW RADIUS Command (Continued)

Parameter	Description
Accounting Port	The accounting protocol port.
Encryption Keys	The server encryption keys, if defined.

Example

This example displays the configuration of the RADIUS client:

```
awplus# show radius
```

SHOW TACACS

Syntax

show tacacs

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the configuration of the TACACS+ client on the switch. An example of the information is shown in Figure 222.

```
TACACS+ Global Configuration
    Timeout            : 5 sec

 Server Host : 149.123.154.12
    Server Status      : Alive
 Server Host : 149.123.154.26
    Server Status      : Dead
```

Figure 222. SHOW TACACS Command

The fields are described in Table 156.

Table 156. SHOW TACACS Command

Parameter	Description
Timeout	The length of the time, in seconds, that the switch waits for a response from a TACACS+ server to an authentication request. The default is 40 seconds. If there is no response from any authentication servers, the switch reactivates the local manager accounts. This parameter cannot be changed.
Server Host	The IP address of a TACACS+ server on your network.

Table 156. SHOW TACACS Command (Continued)

Parameter	Description
Server Status	Indicates the status of the server host. One of the following options is displayed: – Alive: Indicates the server is working correctly. The sockets are successful. – Dead: Indicates the server has timed out or the sockets are unsuccessful.

Example

This example displays the configuration of the TACACS+ client on the switch:

```
awplus# show tacacs
```

TACACS-SERVER HOST

Syntax

```
tacacs-server host ipaddress [key value]
```

Parameters

host

   Specifies an IP address of a TACACS+ server.

key

   Specifies the secret key of a TACACS+ server. The maximum
   length is 40 characters.

Mode

Global Configuration mode

Description

Use this command to add IP addresses of TACACS+ servers to the
TACACS+ client in the switch. The list can have up to three TACACS+
authentication servers, but you can add only one at a time with this
command.

Confirmation Command

"SHOW TACACS" on page 1428

Example

This example adds the IP address 149.11.24.1 to the TACACS+
authentication server list. The server has the key "kenken16:"

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server host 149.11.24.1 order 2 key
kenken16
```

TACACS-SERVER KEY

Syntax

```
tacacs-server key value
```

Parameters

value
> Specifies the global encryption key of the TACACS+ servers. The maximum length is 40 characters.

Mode

Global Configuration mode

Description

Use this command to add the global encryption key of the TACACS+ servers to the TACACS+ client. You can add a global encryption key if you defined one TACACS+ server in the TACACS+ client; or if there is more than one server, and they all use the same encryption key. To define two or three servers that use different encryption keys, do not enter a global encryption key with this command. Instead, define the individual keys when you add the IP addresses of the servers to the client with "TACACS-SERVER HOST" on page 1430.

To remove an existing global key without specifying a new value, use the NO form of this command, NO TACACS-SERVER KEY.

Confirmation Command

"SHOW TACACS" on page 1428

Examples

This example sets the TACACS+ global encryption key to 'key12b':

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server key key12b
```

This example deletes the current TACACS+ global encryption key without defining a new value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server key
```

TACACS-SERVER TIMEOUT

Syntax

```
tacacs-server timeout value
```

Parameters

timeout

Specifies the maximum amount of time the TACACS+ client waits for a response from a TACACS+ authentication server. The range is 1 to 1,000 seconds. The default is 5 seconds.

Mode

Global Configuration mode

Description

Use this command to set the timeout value for the TACACS+ client on the switch. The timeout is the amount of time the client waits for a response from a TACACS+ server for an authentication request. If the timeout expires without a response, the client queries the next server in the list. If there are no further servers in the list to query, the switch defaults to the standard manager and operator accounts.

Use the no form of this command, NO TACACS-SERVER TIMEOUT, to set the TACACS+ timeout to the default value of 5 seconds.

Confirmation Command

"SHOW TACACS" on page 1428

Examples

This example sets the TACACS+ timeout to 55 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server timeout 55
```

This example returns the TACACS+ timeout to the default value of 5 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

1432

Appendix A
System Monitoring Commands

The system monitoring commands are summarized in Table 157 and described in detail within the chapter.

Table 157. System Monitoring Commands

Command	Mode	Description
"SHOW CPU" on page 1434	Privileged Exec	Displays a list of running processes and their CPU utilization.
"SHOW CPU HISTORY" on page 1435	Privileged Exec	Displays graphs of historical CPU utilization of the switch.
"SHOW CPU USER-THREADS" on page 1436	Privileged Exec	Displays a list of CPU utilization and status of the user threads.
"SHOW MEMORY" on page 1437	Privileged Exec	Displays memory consumptions of the processes.
"SHOW MEMORY ALLOCATION" on page 1438	Privileged Exec	Displays the memory allocations used by the processes.
"SHOW MEMORY HISTORY" on page 1439	Privileged Exec	Displays a graph showing historical memory usage.
"SHOW MEMORY POOLS" on page 1440	Privileged Exec	Displays a list of memory pools used by the processes.
"SHOW PROCESS" on page 1441	Privileged Exec	Displays a summary of the current running processes.
"SHOW SYSTEM SERIALNUMBER" on page 1442	User Exec and Privileged Exec	Displays the serial number of the switch.
"SHOW SYSTEM INTERRUPTS" on page 1443	Privileged Exec	Displays the number of interrupts for each Interrupt Request (IRQ) used to interrupt input lines on a Programmable Interrupt Controller (PIC) on the switch.
"SHOW TECH-SUPPORT" on page 1444	Privileged Exec	Stores system information in a file in the file system.

SHOW CPU

Syntax

```
show cpu [sort pri|runtime|sleep|thrds]
```

Parameters

pri

Sorts the list by process priorities.

runtime

Sorts the list by the runtimes of the processes.

sleep

Sorts the list by the average sleeping times.

thrds

Sorts the list by the number of threads.

Mode

Privileged Exec mode

Description

Use this command to display a list of running processes with their CPU utilizations.

Examples

This example lists the running processes by ID numbers:

```
awplus# show cpu
```

This example lists the running processes by runtimes:

```
awplus# show cpu sort runtime
```

1434

SHOW CPU HISTORY

Syntax

```
show cpu history
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display graphs of historical CPU utilization on the switch.

Example

This example displays graphs of historical CPU utilization on the switch:

```
awplus# show cpu history
```

SHOW CPU USER-THREADS

Syntax

```
show cpu user-threads
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display a list of CPU utilization and the status of the user threads.

Example

This example displays a list of CPU utilization and the status of the user threads:

```
awplus# show cpu user-threads
```

SHOW MEMORY

Syntax

```
show memory [sort peak|size|stk]
```

Parameters

peak

Sorts the list by the peak amounts of memory the processes have ever used.

size

Sorts the list by the peak amounts of memory the processes are currently using.

stk

Sorts the list by the stack sizes of the processes.

Mode

Privileged Exec mode

Description

Use this command to display the memory consumption of each process.

Examples

This example displays the memory consumptions of the processes by ID number:

```
awplus# show memory
```

This example displays the memory consumptions by size:

```
awplus# show memory sort size
```

SHOW MEMORY ALLOCATION

Syntax

```
show memory allocation process
```

Parameter

process

Specifies a system process.

Mode

Privileged Exec mode

Description

Use this command to display the memory allocations used by the processes.

Examples

This example displays the memory allocations used by all the processes:

```
awplus# show memory allocation
```

This example displays the memory allocation of the INIT process:

```
awplus# show memory allocation init
```

SHOW MEMORY HISTORY

Syntax

```
show memory history
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display a graph showing historical memory usage.

Example

This example displays a graph showing historical memory usage:

```
awplus# show memory history
```

SHOW MEMORY POOLS

Syntax

```
show memory pools
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display a list of memory pools used by the processes.

Example

This example displays a list of memory pools used by the processes:

```
awplus# show memory pools
```

SHOW PROCESS

Syntax

```
show memory process [sort cpu|mem]
```

Parameters

cpu
  Sorts the list by percentage of CPU utilization.

mem
  Sorts the list by percentage of memory utilization.

Mode

Privileged Exec mode

Description

Use this command to display a summary of the current running processes.

Examples

This example lists the running processes by ID number:

```
awplus# show process
```

This example sorts the list by percentage of CPU utilization:

```
awplus# show process sort mem
```

This example lists the running processes by percentage of memory utilization:

```
awplus# show process sort mem
```

SHOW SYSTEM SERIALNUMBER

Syntax

```
show system serialnumber
```

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display the serial number of the switch. The serial number is also displayed with "SHOW SYSTEM" on page 161.

Example

This example displays the serial number of the switch:

```
awplus# show system serialnumber
```

SHOW SYSTEM INTERRUPTS

Syntax

show system interrupts

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the number of interrupts for each Interrupt Request (IRQ) used to interrupt input lines on a Programmable Interrupt Controller (PIC) on the switch.

Example

This example displays the number of interrupts for each IRQ:

awplus# show system interrupts

SHOW TECH-SUPPORT

Syntax

```
show tech-support [all]
```

Parameters

all

Performs the full set of technical support commands.

Mode

Privileged Exec mode

Description

Use this command to store the system information in a file. You may be asked to perform this command and to send the file to Allied Telesis technical support if you contact the company for assistance with a switch problem. The file is stored in the file system with the file name "tech-support" followed by a string of numbers and the extension "txt." After performing the command, upload the file from the switch using TFTP or Zmodem, and email it to Allied Telesis technical support. For instructions on how to upload files from the switch, refer to "Uploading Files from the Switch with TFTP" on page 493 or "Uploading Files from the Switch with Zmodem" on page 496.

Without the ALL option, the command performs these commands and stores the results in a text file in the file system of the switch:

- ❒ DIR
- ❒ SHOW CLOCK
- ❒ SHOW CPU
- ❒ SHOW FILE SYSTEMS
- ❒ SHOW LOG
- ❒ SHOW MEMORY
- ❒ SHOW PROCESS
- ❒ SHOW RUNNING-CONFIG
- ❒ SHOW STARTUP-CONFIG
- ❒ SHOW SYSTEM
- ❒ SHOW VERSION

1444

With the ALL option, the command performs the previous commands and these additional commands:

❑ SHOW ARP
❑ SHOW INTERFACE
❑ SHOW IP INTERFACE
❑ SHOW IPV6 INTERFACE
❑ SHOW MAC ADDRESS-TABLE

Examples

This example stores the system information in a file:

```
awplus# show tech-support
```

This example performs the full set of technical support commands and stores the system information in a file:

```
awplus# show tech-support all
```

Appendix B

Management Software Default Settings

This appendix lists the factory default settings of the switch. The features are listed in alphabetical order:

❒ "Boot Configuration File" on page 1448

❒ "Class of Service" on page 1449

❒ "Console Port" on page 1450

❒ "802.1x Port-Based Network Access Control" on page 1451

❒ "Enhanced Stacking" on page 1453

❒ "GVRP" on page 1454

❒ "IGMP Snooping" on page 1455

❒ "Link Layer Discovery Protocol (LLDP and LLDP-MED)" on page 1456

❒ "MAC Address-based Port Security" on page 1457

❒ "MAC Address Table" on page 1458

❒ "Management IP Address" on page 1459

❒ "Manager Account" on page 1460

❒ "Port Settings" on page 1461

❒ "RADIUS Client" on page 1462

❒ "Remote Manager Account Authentication" on page 1463

❒ "RMON" on page 1464

❒ "Secure Shell Server" on page 1465

❒ "sFlow Agent" on page 1466

❒ "Simple Network Management Protocol (SNMPv1, SNMPv2c and SNMPv3)" on page 1467

❒ "Simple Network Time Protocol" on page 1468

❒ "Spanning Tree Protocols (STP, RSTP and MSTP)" on page 1469

❒ "System Name" on page 1471

❒ "TACACS+ Client" on page 1472

❒ "Telnet Server" on page 1473

❒ "VLANs" on page 1474

❒ "Web Server" on page 1475

Boot Configuration File

The following table lists the name of the default configuration file.

Boot Configuration File	Default
Switch	boot.cfg

Class of Service

The following table lists the default mappings of the IEEE 802.1p priority levels to the egress port priority queues.

IEEE 802.1p Priority Level	Port Priority Queue
0	Q2
1	Q0 (lowest)
2	Q1
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7 (highest)

Console Port

The following table lists the default settings for the Console port.

Console Port Setting	Default
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Baud Rate	9600 bps

Note
The baud rate is the only adjustable parameter on the port.

1450

802.1x Port-Based Network Access Control

The following table describes the 802.1x Port-based Network Access Control default settings.

802.1x Port-based Network Access Control Settings	Default
Port Access Control	Disabled
Authentication Method	RADIUS EAP
Port Roles	None
Authentication Port	1812

The following table lists the default settings for an authenticator port.

Authenticator Port Setting	Default
Authentication Mode	802.1x
Supplicant Mode	Single
Port Control	Auto
Quiet Period	60 seconds
TX Period	30 seconds
Reauth Enabled	Enabled
Reauth Period	3600 seconds
Supplicant Timeout	30 seconds
Server Timeout	30 seconds
Max Requests	2
VLAN Assignment	Disabled
Control Direction	Both
Guest VLAN	Disabled

The following table lists the default settings for RADIUS accounting.

RADIUS Accounting Settings	Default
Status	Disabled
Port	1813

Enhanced Stacking

The following table lists the enhanced stacking default setting.

Enhanced Stacking Setting	Default
Switch State	Member

GVRP

This section provides the default settings for GVRP.

GVRP Setting	Default
Status	Disabled
GIP Status	Enabled
Join Timer	20 centiseconds
Leave Timer	60 centiseconds
Leave All Timer	1000 centiseconds

IGMP Snooping

The following table lists the IGMP Snooping default settings.

IGMP Snooping Setting	Default
IGMP Snooping Status	Disabled
Multicast Host Topology	Single Host/ Port (Edge)
Host/Router Timeout Interval	260 seconds
Maximum IGMP Multicast Groups	64
Multicast Router Ports Mode	Auto Detect

Link Layer Discovery Protocol (LLDP and LLDP-MED)

The following table lists the default settings for LLDP and LLDP-MED.

LLDP an LLDP-MED	Default
Status	Disabled
Notification Interval	5 seconds
Transmit Interval	30 seconds
Holdtime Multiplier	4
Reinitialization Delay	2 seconds
Transmission Delay Timer	2 seconds
Non-strict MED TLV Order Check	Disabled

MAC Address-based Port Security

The following table lists the MAC address-based port security default settings.

MAC Address-based Port Security Setting	Default
Status	Disabled
Intrusion Action	Protect
Maximum MAC Addresses	No Limit

MAC Address Table

The following table lists the default setting for the MAC address table.

MAC Address Table Setting	Default
MAC Address Aging Time	300 seconds

Management IP Address

The following table lists the default settings for the management IP address.

Management IP Address Setting	Default
Management IP Address	0.0.0.0
Subnet Mask	0.0.0.0
DHCP Client	Disabled

Manager Account

The following table lists the manager account default settings.

Manager Account Setting	Default
Manager Login Name	manager
Manager Password	friend
Console Disconnect Timer Interval	10 minutes
Maximum Number of Manager Sessions	3

Note
Login names and passwords are case sensitive.

1460

Port Settings

The following table lists the port configuration default settings.

Port Configuration Setting	Default
Status	Enabled
10/100/1000Base-T Speed	Auto-Negotiation
Duplex Mode	Auto-Negotiation
MDI/MDI-X	Auto-MDI/MDIX
Threshold Limits for Ingress Packets	Disabled
Broadcast, Multicast, or Unknown Unicast Packet Filtering (Storm-control)	33,554,431 packets per second
Override Priority	No override
Head of Line Blocking Threshold	682 cells
Backpressure	Disabled
Backpressure Threshold	7,935 cells
Flow Control - Send	Disabled
Flow Control - Receive	Disabled
Flow Control Threshold	7,935 cells
Maximum Packet Size	9198 bytes[1]

1. Not adjustable.

RADIUS Client

The following table lists the RADIUS configuration default settings.

RADIUS Configuration Setting	Default
Global Encryption Key	ATI
Global Server Timeout Period	5 seconds
RADIUS Server 1 Configuration	0.0.0.0
RADIUS Server 2 Configuration	0.0.0.0
RADIUS Server 3 Configuration	0.0.0.0
Auth Port	1812
Encryption Key	Not Defined

Remote Manager Account Authentication

The following table describes the remote manager account authentication default settings.

Authentication Setting	Default
Server-based Authentication	Disabled
Active Authentication Method	TACACS+

RMON

The following table lists the default settings for RMON collection histories. There are no default settings for alarms or events.

RMON Setting	Default
History Buckets	50
History Polling Interval	1800 seconds
Owner	Agent
Statistics Groups	None
Events	None
Alarms	None

Secure Shell Server

The following table lists the SSH default settings.

SSH Setting	Default
Status	Disabled
Host Key ID	Not Defined
Server Key ID	Not Defined
Server Key Expiry Time	0 hours
Login Timeout	180 seconds
SSH Port Number	22

Note
The SSH port number is not adjustable.

sFlow Agent

The default settings for the sFlow agent are listed in this table.

sFlow Agent Setting	Default
sFlow Agent Status	Disabled
sFlow Collector IP Address	0.0.0.0
UDP Port	6343
Port Sampling Rate	0
Port Polling Interval	0

Simple Network Management Protocol (SNMPv1, SNMPv2c and SNMPv3)

The following table describes the default settings for SNMPv1, SNMPv2c and SNMPv3.

SNMP Communities Setting	Default
SNMP Status	Disabled
Authentication Failure Trap Status	Disabled

Simple Network Time Protocol

The following table lists the SNTP default settings.

SNTP Setting	Default
System Time	Sat, 01 Jan 2000 00:00:00
SNTP Status	Disabled
SNTP Server	0.0.0.0
UTC Offset	+0
Daylight Savings Time (DST)	Enabled

Spanning Tree Protocols (STP, RSTP and MSTP)

This section provides the default settings for STP and RSTP.

Spanning Tree Status

The following table describes the Spanning Tree Protocol default settings for the switch.

Spanning Tree Setting	Default
Spanning Tree Status	Enabled
Active Protocol Version	RSTP

Spanning Tree Protocol

The following table describes the STP default settings.

STP Setting	Default
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Port Cost	Automatic Update
Port Priority	128

Rapid Spanning Tree Protocol

The following table describes the RSTP default settings.

RSTP Setting	Default
Force Version	RSTP
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Edge Port	Yes
Point-to-Point	Auto Detect
Port Cost	Automatic Update
Port Priority	128

RSTP Setting	Default
Loop Guard	Disabled
BPDU Guard	Disabled
BPDU Guard Timeout Status	Disabled
BPDU Guard Timeout Interval	300 seconds

Multiple Spanning Tree Protocol

The following table describes the RSTP default settings.

MSTP Setting	Default
Force Version	MSTP
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Edge Port	Yes
Point-to-Point	Auto Detect
Port Cost	Automatic Update
Port Priority	128
Loop Guard	Disabled
BPDU Guard	Disabled
BPDU Guard Timeout Status	Disabled
BPDU Guard Timeout Interval	300 seconds

1470

System Name

The default setting for the system name is listed in this table.

System Name Setting	Default
System Name	awplus

TACACS+ Client

The following table lists the TACACS+ client configuration default settings.

TACACS+ Client Configuration Setting	Default
TAC Server 1	0.0.0.0
TAC Server 2	0.0.0.0
TAC Server 3	0.0.0.0
TAC Global Secret	None
TAC Timeout	5 seconds

Telnet Server

The default settings for the Telnet server are listed in this table.

Telnet Server Setting	Default
Telnet Server	Enabled
Telnet Port Number	23

Note
The Telnet port number is not adjustable.

VLANs

This section provides the VLAN default settings.

VLAN Setting	Default
Default VLAN Name	Default_VLAN (all ports)
Management VLAN ID	1 (Default_VLAN)
VLAN Type	Port-based
Member Ports	All Ports
Ingress Filtering	Enabled

Web Server

The following table lists the web server default settings.

Web Server Configuration Setting	Default
Status	Disabled
Operating Mode	HTTP
HTTP Port Number	80
HTTPS Port Number	443

Command Index