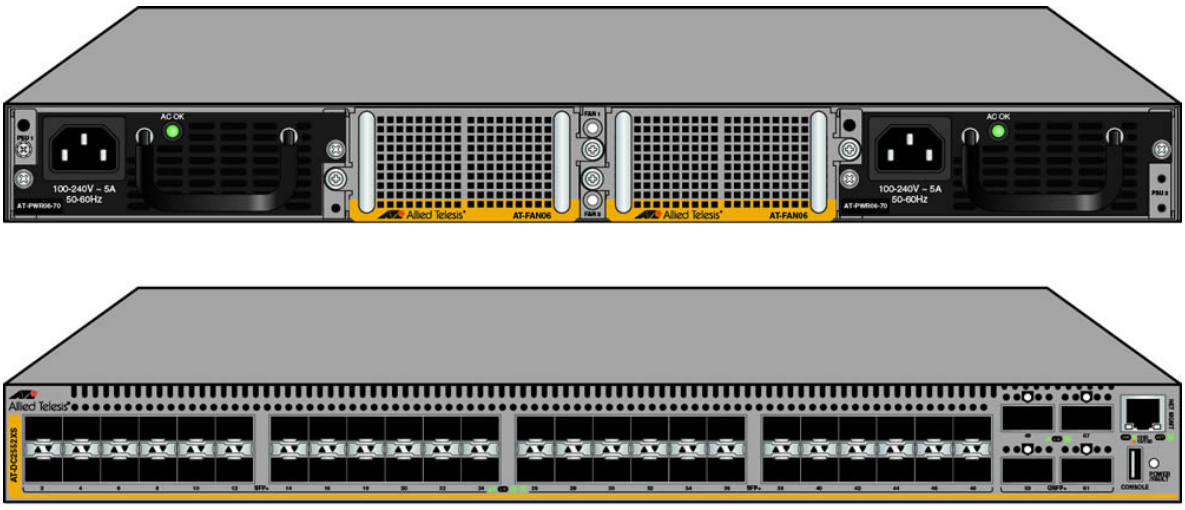
AT-DC2552XS

Layer 2 Data Center Switch



Management Software
Command Line Interface User's Guide

AlliedWare Plus Version 2.5.1.1

613-001753 Rev. A

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

Contents

Tables

Preface

AT-DC2552XS switch is a Layer 2 device that provides 10 and 40 Gigabit Ethernet connectivity for virtualized data center and cloud environments.

This preface contains the following sections:

Caution

The software described in this document may contain certain encryption/security or cryptographic functionality and for exporting those products/software, USA export restrictions apply as per 15 C.F.R. Part 730-772 (particularly Part 740.17). At present, as per United States of America’s export regulations our products/software cannot be exported to Cuba, Iran, North Korea, North Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please refer to export regulations of USA.

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.

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

Switch Management

This section contains the following chapters:

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 management tools from PCs on your network.

Local Management

To access AlliedWare Plus™ command line interface (CLI) locally, the switch has a Console port. This port is located on the rear panel of the DC2552XS switch.

The requirements for local management sessions are a terminal or a PC with a terminal emulator program, and the management cable that comes with the switch.

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

Remote Management

You can remotely manage the switch with these software tools:

- Telnet client
- Secure Shell (SSH) client

To support remote management, you must assign a management IP address to the switch. See “IP ADDRESS” on page 404.

Remote Telnet Management

The switch has a Telnet server that you can use to access AlliedWare Plus™ command line interface (CLI) remotely 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. When an intruder captures the packet with your login name and password, the security of the switch is compromised. For secure remote management, Allied Telesis recommends Secure Shell (SSH).

Remote Secure Shell Management

The switch has an SSH server that you can use to access AlliedWare Plus™ command line interface (CLI) remotely with an SSH client on a management workstation or PCs. This SSH management method is similar to Telnet management sessions. However, SSH management sessions are secure against snooping because the packets are encrypted, rendering them unintelligible to intruders who might capture them.

Manager Account

You must log on to manage the switch. This requires a valid user name and password. The switch comes with one 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.

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.

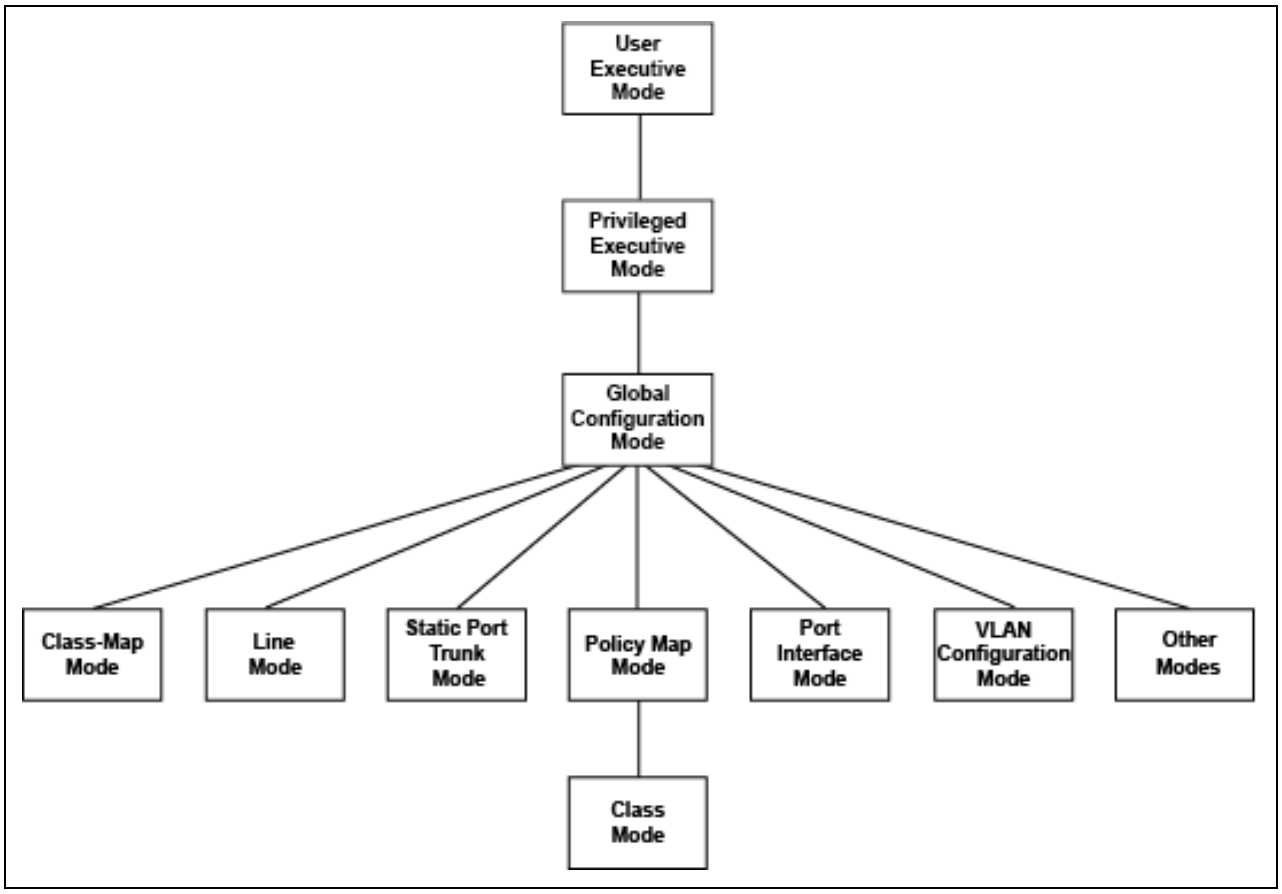


Figure 1. Command Modes

The modes have different commands and support different management functions. To perform a management function, you first have to move to the mode that has the appropriate commands. For instance, to add new VLANs, you must move to the VLAN Configuration mode because the VLAN command is effective only in that mode.

Moving Down the Hierarchy

To move down the mode hierarchy, you must step through each mode in sequence.

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. Here are some examples.

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

CLASS-MAP Command

You use this command to move from the Global Configuration mode to the Class-Map mode in which you create classifiers and flow groups for Quality of Service policies. The format of the command is:

```
class-map class_name
```

```
awplus(config)# class-map filecopy
awplus(config-cmap)#
```

Figure 4. CLASS-MAP 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 5. LINE CONSOLE Command

Moving Up the Hierarchy

Four commands are available 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 of the modes. They move you up one level in the hierarchy, as illustrated in Figure 6.

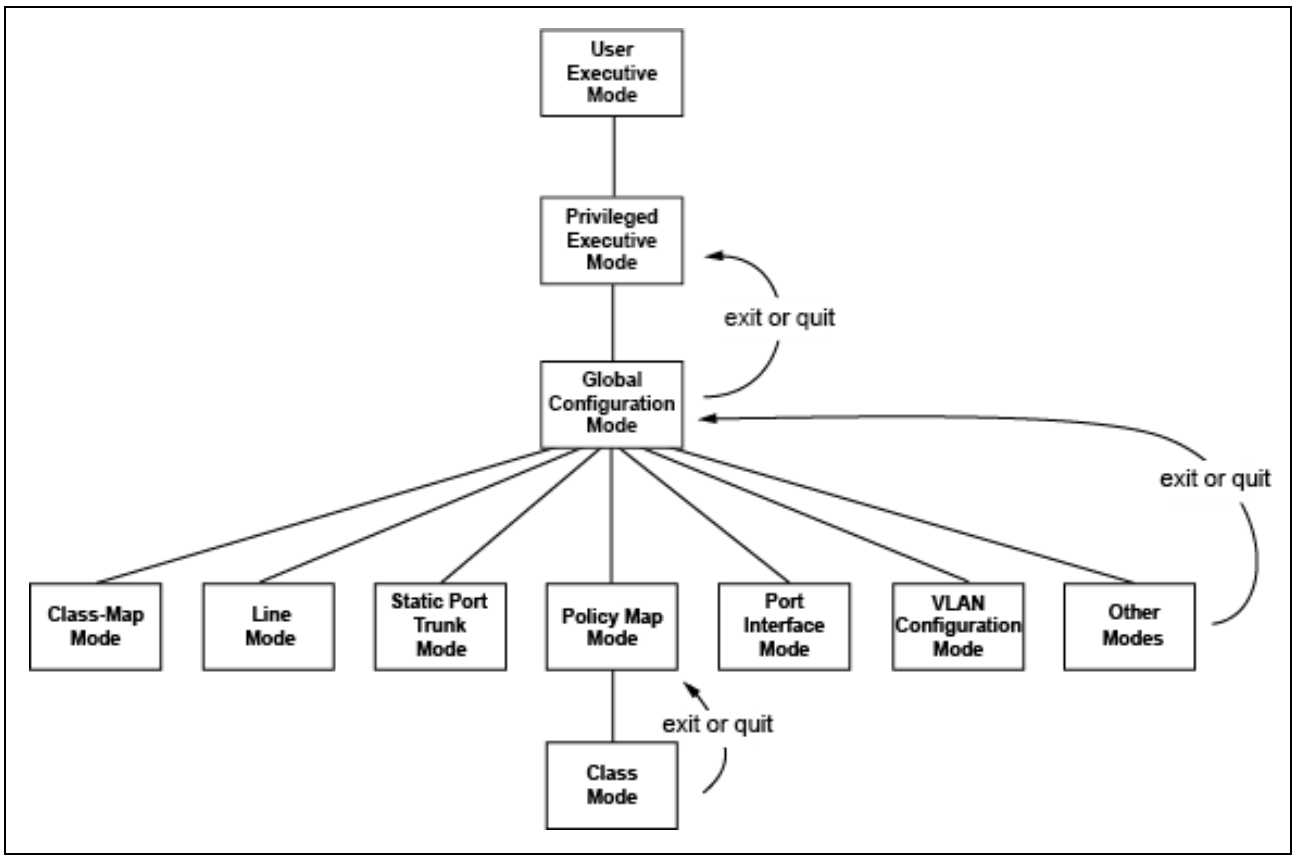


Figure 6. Moving Up One Mode with the EXIT and QUIT Command

END Command

You may want to return to the User Exec mode or the Privileged Exec mode after you have configured a feature. While you can step back through the modes one at a time with the EXIT or QUIT command, the END command moves you directly to the Privileged Exec mode from any mode below the Global Configuration mode.

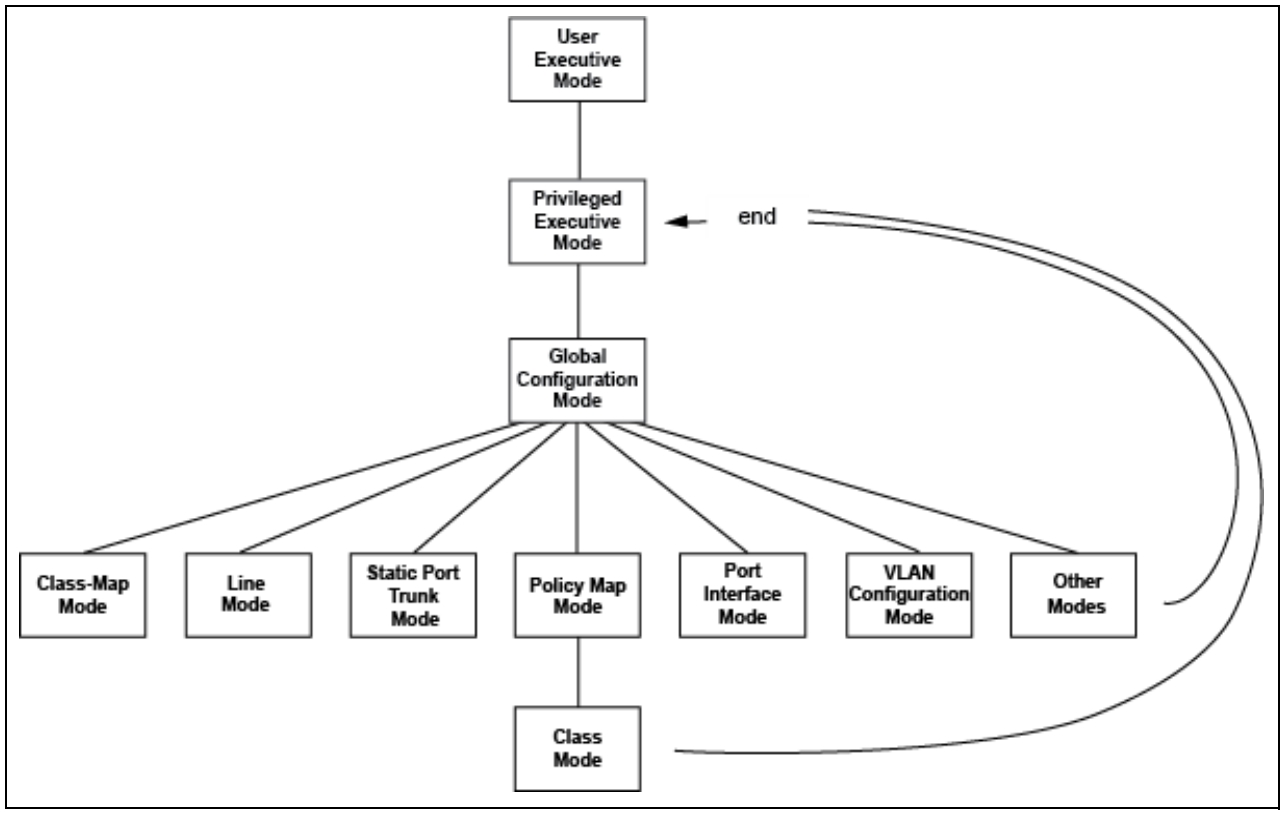


Figure 7. Returning to the Privileged Exec Mode with the END Command

DISABLE Command

To return to the User Exec mode from the Privileged Exec mode, use the DISABLE command.

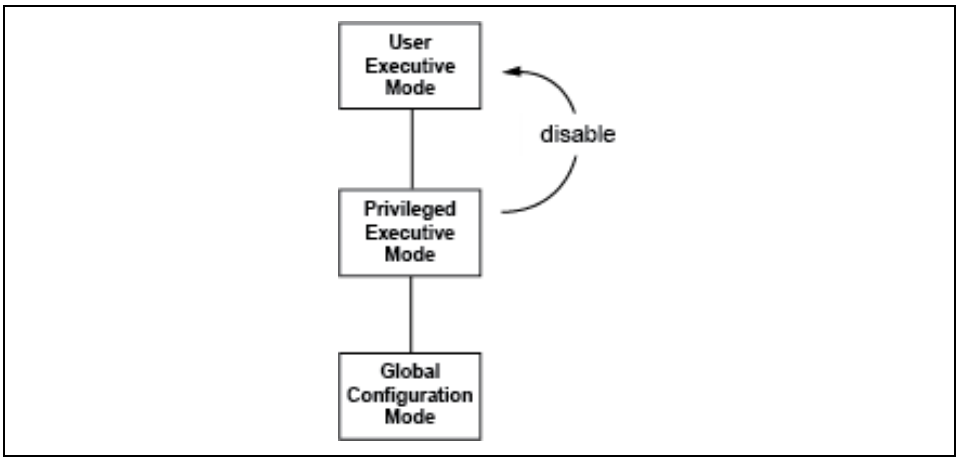


Figure 8. Returning to the User Exec Mode with the DISABLE Command

Port ID Numbers in Commands

Here is the format for port ID numbers in commands:

`port1.0.`*n*

The *n* variable is the number of the port you want to configure on the switch. The two digits in the prefix “port1.0.” are used with modular products and with products that support stacking. To specify a port number on the DC2552XS switch, which is not a modular product and does not support stacking, you must always use the prefix “port1.0.”

This example uses the INTERFACE PORT command to enter the Port Interface mode for ports 1.0.12 and 1.0.18:

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

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 or keywords.
- | - Vertical line separates parameter or keyword options for you to choose from.
- *Italics* - Italics indicate variables you 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 three new VLANs with VIDs 10, 20, and 30:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 10,20,30
awplus(config-vlan)# exit
```

Chapter 2

Management Session Commands

The management session commands are summarized in Table 1.

Table 1. Management Session Commands

Command	Mode	Description
“BAUD-RATE SET” on page 36	Global Configuration	Sets the baud rate of the Console port.
“CLEAR LINE” on page 37	Privileged Exec	Ends a remote management session on another line.
“CRYPTO KEY DESTROY HOSTKEY” on page 38	Global Configuration	Deletes an encryption key pair for the SSH server.
“CRYPTO KEY GENERATE HOSTKEY” on page 40	Global Configuration	Creates or updates an encryption key pair for the SSH server.
“EXEC-TIMEOUT” on page 42	Console Line and Virtual Terminal Line	Sets the management session timers.
“LENGTH” on page 44	Console Line and Virtual Terminal Line	Sets the maximum number of lines that the SHOW commands display on the screen for local and remote management sessions.
“LINE CONSOLE 0” on page 46	Global Configuration	Enters the Console Line mode.
“LINE VTY” on page 47	Global Configuration	Enters the Virtual Terminal Line mode.
“NO EXEC-TIMEOUT” on page 48	Console Line and Virtual Terminal Line	Resets the management session timers to 10 minutes.
“NO LENGTH” on page 49	Console Line and Virtual Terminal Line	Resets the maximum number of lines the SHOW commands display on the screen to 20 lines for local and remote management sessions.
“NO SERVICE SSH” on page 50	Global Configuration	Disables the SSH server on the switch.

Table 1. Management Session Commands (Continued)

Command	Mode	Description
“NO SERVICE PASSWORD-ENCRYPTION” on page 51	Global Configuration	Disables password encryption.
“NO SERVICE TELNET” on page 52	Global Configuration	Disables the Telnet server on the switch.
“NO SERVICE TERMINAL-LENGTH” on page 53	Global Configuration	Resets the maximum number of lines that the SHOW commands display on the screen at once to the default value of 20 lines.
“NO USERNAME” on page 54	Global Configuration	Deletes manager accounts from the switch.
“SERVICE MAXMANAGER” on page 55	Global Configuration	Specifies the maximum number of management accounts with a user level of 15 that the switch allows to log on to the switch at once.
“SERVICE PASSWORD-ENCRYPTION” on page 56	Global Configuration	Encrypts all manager account passwords that are stored in the running configuration file.
“SERVICE SSH” on page 57	Global Configuration	Enables the SSH server on the switch.
“SERVICE TELNET” on page 58	Global Configuration	Enables the Telnet server on the switch.
“SERVICE TERMINAL-LENGTH” on page 59	Global Configuration	Specifies the maximum number of lines that the SHOW commands display on the screen at once.
“SHOW BAUD-RATE” on page 60	User Exec	Displays the settings of the Console port.
“SHOW CRYPTO KEY HOSTKEY” on page 62	Privileged Exec and Global Configuration	Displays the encryption keys for the SSH server.
“SHOW SSH SERVER” on page 63	User Exec and Privileged Exec	Displays the status of the SSH server on the switch.
“SHOW TELNET” on page 64	User Exec and Privileged Exec	Displays the status of the Telnet server on the switch.
“SHOW USERS” on page 65	Privileged Exec	Displays the managers who are currently logged on the switch.

Table 1. Management Session Commands (Continued)

Command	Mode	Description
"TERMINAL LENGTH" on page 67	User Exec	Specifies the maximum number of lines that the SHOW commands display on the screen in your current session.
"TERMINAL NO LENGTH" on page 68	User Exec	Resets the maximum number of lines that the SHOW commands display on the screen to 20 lines in your current session.
"TELNET" on page 69	Privileged Exec	Starts Telnet management sessions on network devices.
"USERNAME" on page 70	Global Configuration	Creates new manager accounts.

BAUD-RATE SET

Syntax

```
baud-rate set baud_rate
```

Parameter

baud_rate
: Specifies the baud rate of the Console port in bps. The options are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

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. After changing the baud rate of the Console port, change the baud rate of the Console terminal. These two baud rates must be the same.

Confirmation Command

“SHOW BAUD-RATE” on page 60

Example

This example sets the baud rate of the Console port to 9600 bps:

```
awplus> enable
awplus# configure terminal
awplus(config)# baud-rate set 9600

Baud rate changed to 9600 bps.
Change your console baud correspondingly.

awplus(config)#
```

CLEAR LINE

Syntax

```
clear line line_number
```

Parameter

line_number
: Specifies the line number of a remote Telnet or SSH management session. The line number ranges from 0 to 9.

Mode

Privileged Exec mode

Description

Use this command to log out of a specific remote Telnet or SSH management session on another line. To view the line numbers, see the Line Field in the SHOW USERS commands. The value of the line_number parameter is the value of N in "vty*N*." See "SHOW USERS" on page 65.

Confirmation Command

"SHOW USERS" on page 65

Example

This example ends a remote management session on vty 0:

```
awplus> clear line 0
```

CRYPTO KEY DESTROY HOSTKEY

Syntax

```
crypto key destroy hostkey dsa|rsa|rsa1
```

Parameters

dsa
: Deletes the DSA host key in SSH protocol version 2.

rsa
: Deletes the RSA host key in SSH protocol version 2.

rsa1
: Deletes the RSA1 host key in SSH protocol version 1.

Mode

Global Configuration mode

Confirmation Command

“SHOW CRYPTO KEY HOSTKEY” on page 62

Description

Use this command to delete an encryption key pair for the SSH server. The encryption keys are stored in files in Flash memory on the switch. This command deletes the files directly from the Flash memory so that you do not have to enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command to save your changes.

See Table 2 for the file names associated with the encryption keys.

Table 2. SHOW BAUD-RATE Command

Keyword	FIle Names
dsa	ssh_host_dsa_key, ssh_host_dsa_key.pub
rsa	ssh_host_rsa_key, ssh_host_rsa_key.pub
rsa1	ssh_host_key, ssh_host_key.pub

Example

This example deletes the DSA key:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key destroy hostkey dsa
```

CRYPTO KEY GENERATE HOSTKEY

Syntax

```
crypto key generate hostkey dsa|rsa|rsa1 [key_length]
```

Parameters

`dsa`
: Creates a DSA key pair in SSH protocol version 2.

`rsa`
: Creates an RSA key pair in SSH protocol version 2.

`rsa1`
: Creates an RSA1 key pair in SSH protocol version 1.

`key_length`
: Specifies the length of the encryption key, in bits, for the RSA key. This parameter is valid only when you specify the RSA key. The range is 768 to 2,048 bits. If you do not specify this parameter for the RSA key, the key length of the RSA key is 1024 bits. The DSA and RSA1 keys have fixed lengths of 1024 bits.

Mode

Global Configuration mode

Confirmation Command

“SHOW CRYPTO KEY HOSTKEY” on page 62

Description

Use this command to create or update an encryption key pair for the SSH server. You must create at least one encryption key pair before enabling the sever. The switch can have one key pair of each type, DSA, RSA, and RSA1, 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.

When the switch does not have an RSA1 key pair for SSH protocol version 1, you cannot connect to the switch in SSH protocol version 1. Similarly, when the switch does not have either a DSA or RSA key pair for SSH protocol version 2, you cannot connect to the switch in SSH protocol version 2.

A new encryption key is saved in the Flash memory of the switch when you enter the command. After entering this command, you do not have to enter WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command to save your changes on the switch.

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
```

EXEC-TIMEOUT

Syntax

```
exec-timeout value
```

Parameter

value
: Specifies the session timer in minutes. The range is 0 to 35,791 minutes. Assign a value of 0 if you do not want to time out a session. The default value is 10 minutes.

Modes

Console Line 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. The switch deems a management session inactive when a management session has no 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. To set the timer for local management sessions, enter the command in the Line Console mode. To set the timers for remote Telnet and SSH sessions, enter the command in the Virtual Terminal Line mode.

Confirmation Command

“SHOW SWITCH” on page 117

Examples

This example sets the session timer for local management sessions to 0 minutes which indicates to not time out sessions:

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

This example sets the timer for remote management sessions to 3 minutes:

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

LENGTH

Syntax

```
length length
```

Parameter

length

Specifies the maximum number of lines that the SHOW commands display on the screen at once. The range is 0 to 512 lines. Assign a value of 0 if you do not want the SHOW commands to pause. The default value is 20 lines.

Mode

Console Line and Virtual Terminal Line modes

Description

Use this command to specify the maximum number of lines that the SHOW commands display on the screen at once. You can set different values for the local and remote management sessions with this command.

- For local management sessions, enter the command in the Console line mode.
- For remote Telnet and SSH sessions, enter the command in the Virtual Terminal Line (VTY) mode.

If the maximum numbers of lines are set by the TERMINAL LENGTH or SERVICE TERMINAL-LENGTH command, the switch uses these settings to display output. Here is the priority of the commands, listing the highest priority command first:

1. The TERMINAL LENGTH command
2. The SERVICE TERMINAL-LENGTH command
3. The LENGTH command

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

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 the Telnet and SSH sessions:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0 9
awplus(config-line)# length 15
```

LINE CONSOLE 0

Syntax

```
line console 0
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enter the Console Line mode.

Example

This example enters the Console Line mode:

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

LINE VTY

Syntax

```
line vty line_id [ending_line_id]
```

Parameters

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

ending_line_id
Specifies the last number of a VTY line that you want to configure. The range is 0 to 9.

Mode

Global Configuration mode

Description

Use this command to enter the Virtual Terminal Line mode for a VTY line. Commands that are entered in the VTY Line mode apply to a group of the VTY lines with the range beginning with line_id value and ending with ending_line_id value.

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 multiple VTY lines, from VTY 0 to VTY 9:

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

NO EXEC-TIMEOUT

Syntax

```
no exec-timeout
```

Parameters

None

Modes

Console Line and Virtual Terminal Line modes

Description

Use this command to reset the management session timers to 10 minutes.

Confirmation Command

“SHOW SWITCH” on page 117

Example

This example sets the session timer for local management sessions to 10 minutes:

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

NO LENGTH

Syntax

```
no length
```

Parameters

None

Mode

Console Line and Virtual Terminal Line modes

Description

Use this command to reset the maximum number of lines that the SHOW commands display at once to the default value of 20 lines. You can apply this setting to local and remote management sessions.

Confirmation Command

"SHOW SWITCH" on page 117

Examples

This example resets the maximum number of lines to display to the default value, 20 lines, for local management sessions:

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

This example resets the maximum number of lines to display to the default value, 20 lines, for remote management sessions:

```
awplus> enable
awplus# configure terminal
awplus(config)# line vty 0 9
awplus(config-line)# no length
```

NO SERVICE SSH

Syntax

```
no service ssh
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the SSH server on the switch. By default, the SSH server is disabled.

Confirmation Command

“SHOW SSH SERVER” on page 63

Example

This example disables the SSH server:

```
awplus(config)# no service ssh
```

NO SERVICE PASSWORD-ENCRYPTION

Syntax

```
no service password-encryption
```

Parameters

None.

Mode

Global Configuration mode

Description

Use this command to disable password encryption. Passwords originally defined in plain text are displayed in plain text in the running-config file. However, encrypted passwords stay encrypted in the running-config file even after this command is issued. Passwords originally entered in plain text and then encrypted and saved in the startup-config file remain encrypted.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

The following example disables password encryption:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service password-encryption
```

NO SERVICE TELNET

Syntax

```
service telnet
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the Telnet server on the switch. By default, the Telnet server is enabled.

Confirmation Command

“SHOW TELNET” on page 64

Example

This example disables the Telnet server:

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

NO SERVICE TERMINAL-LENGTH

Syntax

```
no service terminal-length
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to reset the maximum number of lines that the SHOW commands display on the screen at once to the default value of 20 lines.

Example

This example resets the maximum number of lines to the default value of 20 lines:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service terminal-length
```

NO USERNAME

Syntax

```
no username name
```

Parameter

name
: Specifies the name of the manager account. The name is case-sensitive.

Mode

Global Configuration mode

Description

Use this command to delete local manager accounts from the switch. You can delete the default “manager” account from the switch as well.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example deletes the manager account “msmith”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no username msmith
```

SERVICE MAXMANAGER

Syntax

```
service maxmanager value
```

Parameter

value
: Specifies the maximum number of management accounts with a user level of 15 that the switch allows to be open at once. The range is 1 to 3. The default is 3.

Mode

Global Configuration mode

Description

Use this command to set the maximum number of management accounts with a user level of 15 that the switch allows to log on to the switch simultaneously. Management accounts with a user level of 15 have unrestricted access to the management software.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example permits only one management account, with a user level of 15, to log on to the switch at one time:

```
awplus(config)# service maxmanager 1
```

SERVICE PASSWORD-ENCRYPTION

Syntax

```
service password-encryption
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to encrypt all manager account passwords and the value assigned to the ENABLE PASSWORD in all configuration files on the switch. By default, passwords are stored in encrypted form in configuration files. For more information about the ENABLE PASSWORD command, see “ENABLE PASSWORD” on page 80.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example encrypts all manager account passwords and the value of the ENABLE PASSWORD command in all configuration files on the switch:

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

SERVICE SSH

Syntax

```
service ssh
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the SSH server on the switch so that you can manage the switch remotely with the SSH protocol. By default, the SSH server is disabled.

Before enabling the SSH server, you must create at least one encryption key for the SSH server using the "CRYPTO KEY GENERATE HOSTKEY" on page 40.

Confirmation Command

"SHOW SSH SERVER" on page 63

Example

This example enables the SSH server:

```
awplus(config)# service ssh
```

SERVICE TELNET

Syntax

```
service telnet
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the Telnet server on the switch so that you can manage the switch remotely with the Telnet protocol. By default, the Telnet server is enabled.

Confirmation Command

“SHOW TELNET” on page 64

Example

This example enables Telnet server:

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

SERVICE TERMINAL-LENGTH

Syntax

```
service maxmanager length
```

Parameter

length

Specifies the maximum number of lines that the SHOW commands display on the screen at once. The range is 0 to 512 lines. Use the value 0 if you do not want the SHOW commands to pause. The default value is 20 lines.

Mode

Global Configuration mode

Description

Use this command to specify the maximum number of lines that the SHOW commands display on the screen at once.

If the maximum number of lines is set by the TERMINAL LENGTH command, the switch uses that setting to displays output. Here is the priority of the commands, listing the highest priority command first:

1. The TERMINAL LENGTH command
2. The SERVICE TERMINAL-LENGTH command
3. The LENGTH command

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example sets the maximum number of lines to 30:

```
awplus> enable
awplus# configure terminal
awplus(config)# service terminal-length 30
```

SHOW BAUD-RATE

Syntax

```
show baud-rate
```

Parameters

None

Mode

User Exec mode

Description

Use this command to display the Console port settings, which are used for local management sessions on the switch. See Figure 9 for an example of the command output.

```
Asynchronous Port (Console) Information:
   Baud Rate ..................... 115200
   Parity ........................ None
   Data bits ..................... 8
   Stop bits ..................... 1
```

Figure 9. SHOW BAUD-RATE Command

The fields are described in Table 3.

Table 3. SHOW BAUD-RATE Command

Field	Description
Baud Rate	Displays the speed of the data transmission in bps on the Console port.
Parity	Displays the type of parity checking. It is always is set to “None.”
Data bits	Displays the length of data bits. It is always set to “8.”
Stop bits	Displays the length of stop bits. It is always set to “1.”

Note
The Baud Rate is the only adjustable parameter on the Console port.

Example

This example displays the Console port settings:

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

SHOW CRYPTO KEY HOSTKEY

Syntax

```
show crypto key hostkey [dsa|rsa|rsa1]
```

Parameters

`dsa`
Displays the DSA key pair.

`rsa`
Displays the RSA key pair.

`rsa1`
Displays the RSA1 key pair.

Modes

Privileged Exec and Global Configuration modes

Description

Use this command to display the encryption keys. See Figure 10 for an example of the command output.

```
Type  Bits    Fingerprint
-----------------------------------------------------

RSA1  1024    62:72:40:cd:e6:61:55:c0:47:2b:0d:3b:69:a1:0a:06

RSA   1024    8a:50:a5:a0:c8:7b:7d:2f:ab:b2:80:8a:b2:d0:1f:bb

DSA   1024    a3:9c:c6:97:28:ce:89:e7:30:a7:07:d2:bf:53:b0:d0
```

Figure 10. SHOW CRYPTO KEY HOSTKEY Command

Examples

This example displays the encryption 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

User Exec mode and Privileged Exec mode

Description

Use this command to display the status of the SSH server on the switch. The status of the SSH server can be either enabled or disabled. See Figure 11 for an example of the command output.

```
Secure Shell Server Configuration
Versions Supported .......... 2,1
SSH Server:   Enabled
Server Port ................. 22
```

Figure 11. SHOW SSH SERVER Command

The fields are described in Table 4.

Table 4. SHOW BAUD-RATE Command

Field	Description
Versions Supported	Displays the enabled SSH versions.
SSH Server	Displays whether the SSH server is enabled or disabled.
Server Port	Displays the TCP port number of the SSH server.

Example

This example displays the status of the SSH server on the switch:

```
awplus# show ssh server
```

SHOW TELNET

Syntax

```
show telnet
```

Parameters

None

Modes

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 Telnet server can be either enabled or disabled. See Figure 12 for an example of the command output.

```
Telnet Server Configuration
---------------------------------------------------------
Telnet Server: Enabled
```

Figure 12. SHOW TELNET Command

Example

This example displays the status of the Telnet server on the switch:

```
awplus# show telnet
```

SHOW USERS

Syntax

```
show users
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the managers who are currently logged onto the switch. See Figure 13 for an example of the output.

```
Line  User      Host(s)      Idle          Location
con0  manager   idle         00:00:00      ttyS0
vty0  manager   idle         00:01:25      172.17.28.70
vty1  manager   idle         00:04:06      172.17.28.71
```

Figure 13. SHOW USERS Command

The columns are described in Table 5.

Table 5. SHOW USERS Command

Field	Description
Line	Indicates an active management session. The possible designators are: ❒ con0: a local management session. ❒ vty*N*: a remote Telnet and SSH session where *N* is a number that is assigned to the session.
User	Indicates the user name that is logged into the account.
Host(s)	Not supported.
Idle	Indicates the idling time.
Location	Indicates 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.

Example

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

```
awplus# show users
```

TERMINAL LENGTH

Syntax

```
terminal length length
```

Parameter

length

Specifies the maximum number of lines that the SHOW commands display on the screen at once. The range is 0 to 512 lines. Assign a value of 0 if you do not want the SHOW commands to pause. The default value is 20 lines.

Mode

User Exec mode

Description

Use this command to specify the maximum number of lines that the SHOW commands display on the screen at once in your current session. The setting of this command is effective *only* for your current session and is not stored in the running configuration. This command overrides the settings by the SERVICE TERMINAL-LENGTH and LENGTH commands.

Confirmation Command

None

Example

This example sets the maximum number of lines to 30 for your current session:

```
awplus> enable
awplus# terminal length 30
```

TERMINAL NO LENGTH

Syntax

```
terminal no length
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to reset the maximum number of lines that the SHOW commands display on the screen at once to the default value of 20 lines in your current session.

Confirmation Command

None

Example

This example resets the maximum number of lines to the default value of 20 lines:

```
awplus(config)# terminal no length
```

TELNET

Syntax

```
telnet ipv4_address
```

Parameter

ipv4_address
: Specifies the IPv4 address of a remote device you want to manage using the Telnet client on the switch.

Mode

Privileged Exec mode

Description

Use this command to start a Telnet management session on a network device that has an IPv4 address. You can manage one remote device at a time.

Example

This example starts a Telnet management session on a network device that has an IP address of 10.0.0.10:

```
awplus> enable
awplus# telnet 10.0.0.10
```

USERNAME

Syntax

`username` *`name`* `[privilege 1|15] password [8]` *`password`*

Parameters

`name`

Specifies the name of a new manager account or existing manager account. The name is case-sensitive and can be up to 15 alphanumeric characters. Spaces and special characters are not permitted.

`privilege`

Specifies this keyword to assign the privilege level of either 1 or 15, or modify the privilege level. If you do not specify the privilege level when creating a new account, the privilege level of the new account is set to 1 automatically. If you do not specify the privilege level when modifying an existing account, the existing account's privilege level remains the same.

1

Specifies a manager account with the privilege level of 1. A manager account with the privilege level of 1 is restricted to the User Exec mode when command mode restriction is activated with the ENABLE PASSWORD command. However, a manager account with the privilege level of 1 can move to the Privileged Exec mode if the user enters the correct password.

15

Specifies a manager account with the privilege level of 15. A manager account with the privilege level of 15 has access to all modes.

`password`

Assigns a new password or modifies an existing password. You must set the password when creating a new account. The password setting is optional when you modify an existing account. If you do not specify a password when modifying an existing account, the existing account's password stays the same.

8

Specifies that the password is encrypted.

password

Specifies the password of the new manager account. A password is case-sensitive and can be up to 16 alphanumeric characters. Special characters are permitted with the exception of spaces, exclamation points (!), and question marks (?).

Mode

Global Configuration mode

Description

Use this command to create a new manager account or modify the password and privilege levels of an existing manager account.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example creates a manager account with the user name "allen." The privilege level is 15 provides the manager access to all modes even when 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
```

Chapter 3

Basic Command Line Management Commands

The basic command line commands are summarized in Table 6.

Table 6. Basic Command Line Commands

Command	Mode	Description
“CLEAR SCREEN” on page 75	User Exec and Privileged Exec	Clears the screen.
“CONFIGURE TERMINAL” on page 76	Privileged Exec	Moves you from the Privileged Exec mode to the Global Configuration mode.
“DISABLE” on page 77	Privileged Exec	Returns you to the User Exec mode from the Privileged Exec mode.
“DO” on page 78	Global Configuration	Performs Privileged Exec mode commands from the Global Configuration mode.
“ENABLE” on page 79	User Exec	Moves you from the User Exec mode to the Privileged Exec mode.
“ENABLE PASSWORD” on page 80	Global Configuration	Specifies the password which permits management accounts with a privilege level of 1 an option to move to the Privilege Exec mode.
“END” on page 81	All modes below the Global Configuration mode	Returns you to the Privileged Exec mode.
“EXIT” on page 82	All modes except the User Exec and Privileged Exec	Moves you up one mode.
“LOGOUT” on page 83	User Exec	Ends a management session.
“NO ENABLE PASSWORD” on page 84	Global Configuration	Removes the password which permits management accounts with a privilege level of 1 to move to the Privilege Exec mode.

Table 6. Basic Command Line Commands (Continued)

Command	Mode	Description
“QUIT” on page 85	All modes except the User Exec and Privileged Exec	Moves you up one mode.

CLEAR SCREEN

Syntax

```
clear screen
```

Parameters

None

Modes

User Exec mode

Description

Use this command to clear the screen.

Example

This example clears the screen:

```
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

This example moves you from the Privileged Exec mode to the Global Configuration mode:

```
awplus# configure terminal
awplus(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.

To move from the User Exec mode to the Privileged Exec mode, see "ENABLE" on page 79.

Example

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

```
awplus# disable
awplus>
```

DO

Syntax

do *command*

Parameter

command
Specifies the command to perform in the Privileged Exec mode.

Mode

Global Configuration mode and modes below the Global Configuration mode

Description

Use this command to perform Privileged Exec mode commands from the Global Configuration mode, or modes below the Global Configuration mode, such as, the Line, Port Interface, VLAN Configuration modes. You may use the command to perform some, but not all, of the Privileged Exec mode commands.

Examples

This example performs the SHOW INTERFACE command for port 1.0.4 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. To return to the User Exec mode, see "DISABLE" on page 77.

Example

This example moves management accounts with a privilege level of 15 from the User Exec mode to the Privileged Exec mode:

```
awplus> enable
awplus#
```

ENABLE PASSWORD

Syntax

`enable password [8] password`

Parameters

8
: Specifies that the password is encrypted.

password
: Specifies a password. A plaintext password is case-sensitive and can have up to 16 alphanumeric characters including special characters. Spaces are *not* permitted.

Mode

Global Configuration mode

Description

Use this command to specify a password to enable management accounts with a privilege level of 1 to move to the Privilege Exec mode from the User Exec mode. By default, the password is not specified and management accounts with a privilege level of 1 are restricted to the User Exec mode.

For management accounts with privilege level 1 to move to the Privilege Exec mode from the User Exec mode, you must set a password with this command. Then you must enter this password with the ENABLE command.

Note
Management accounts with a privilege level of 15 are permitted to move to the Privilege Exec mode without entering a password.

Confirmation Command

show running-config

Example

This example specifies the password as "x8pgHUdh":

```
awplus> enable
awplus# configure terminal
awplus# enable password x8pgHUdh
```

END

Syntax

```
end
```

Parameters

None

Mode

All modes below the Global Configuration mode.

Description

Use this command to return to the Privileged Exec mode.

The shortcut key of the END command is Ctrl-Z.

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 up 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.

The shortcut key of the EXIT command is Ctrl-D.

Example

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

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

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. See "EXIT" on page 82.

Example

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

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

NO ENABLE PASSWORD

Syntax

```
no enable password
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to remove the password that permits management accounts with a privilege level of 1 to move to the Privilege Exec mode from the User Exec mode.

Note
Management accounts with a privilege level of 15 are permitted to move to the Privilege Exec mode without entering a password and are not affected by this command.

Confirmation Command

show running-config

Example

This example removes the password to permit management accounts with a privilege level of 1 to move to the Privilege Exec mode:

```
awplus> enable
awplus# configure terminal
awplus# no enable password
```

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 similar to the EXIT command. The difference is that unlike the EXIT command, the QUIT command cannot be used to end a management session.

The shortcut key of the QUIT command is Ctrl-D.

Example

This example moves you from the Global Configuration mode to the Privileged Exec mode:

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

Chapter 4

Basic Switch Operations Commands

The basic switch operations commands are summarized in Table 7.

Table 7. Basic Switch Operations Commands

Command	Mode	Description
“BANNER EXEC” on page 89	Global Configuration	Creates a User Exec and Privileged Exec modes banner.
“BANNER LOGIN” on page 90	Global Configuration	Creates a login banner.
“BANNER MOTD” on page 91	Global Configuration	Creates a message-of-the-day banner.
“BOOT SYSTEM” on page 92	Global Configuration	Specifies a management software image file that the switch uses when the system is rebooted or reloaded.
“CLOCK SET” on page 93	Privileged Exec	Manually sets the date and time.
“ERASE STARTUP-CONFIG” on page 95	Privileged Exec	Deletes the boot configuration file to restore the default settings.
“HOSTNAME” on page 96	Global Configuration	Assigns a name to the switch.
“NO BANNER EXEC” on page 97	Global Configuration	Deletes the banner message.
“NO BANNER LOGIN” on page 98	Global Configuration	Deletes the banner login message.
“NO BANNER MOTD” on page 99	Global Configuration	Deletes the banner message-of-the-day.
“NO HOSTNAME” on page 100	Global Configuration	Deletes the switch’s name without assigning a new name.
“REBOOT” on page 101	Privileged Exec	Resets the switch.
“RELOAD” on page 102	Privileged Exec	Resets the switch.
“SHOW BOOT” on page 103	Privileged Exec	Displays information about the management software and configuration file.

Table 7. Basic Switch Operations Commands (Continued)

Command	Mode	Description
“SHOW CLOCK” on page 105	User Exec and Privileged Exec	Displays the date and time.
“SHOW CPU” on page 106	Privileged Exec	Displays a list of running processes with their CPU utilization.
“SHOW CPU HISTORY” on page 109	Privileged Exec	Displays graphs of historical CPU utilization.
“SHOW MEMORY” on page 110	Privileged Exec	Displays the memory consumption of each process.
“SHOW MEMORY HISTORY” on page 112	Privileged Exec	Displays graphs of historical memory utilization.
“SHOW PROCESS” on page 113	Privileged Exec	Displays a list of running processes with their CPU utilization.
“SHOW RUNNING-CONFIG” on page 116	Privileged Exec	Displays the settings of the switch.
“SHOW SWITCH” on page 117	Privileged Exec	Displays general information about the switch.
“SHOW SYSTEM” on page 119	Privileged Exec	Displays general information about the switch.
“SHOW SYSTEM ENVIRONMENT” on page 122	Privileged Exec	Displays detailed information about the switch, PSUs, and fan modules.
“SHOW SYSTEM PLUGGABLE” on page 124	Privileged Exec	Displays information about the SFP+ and QSFP+ modules.
“SHOW SYSTEM PLUGGABLE DETAIL” on page 126	Privileged Exec	Displays detailed information about the SFP+ QSFP+ modules.
“SHOW SYSTEM SERIALNUMBER” on page 128	Privileged Exec	Displays the serial number of the switch.
“SHOW TECH-SUPPORT” on page 129	Privileged Exec	Generates a debug log file.
“SHOW VERSION” on page 130	Privileged Exec	Displays the versions and build dates of the management software and bootloader.

BANNER EXEC

Syntax

```
banner exec [default]
```

Parameter

`default`
: Specifies the banner as a default setting, which is the firmware version number and the host name of the switch.

Mode

Global Configuration mode

Description

Use this command to create a banner that is displayed right after you log on or clear the screen with the CLEAR SCREEN command.

After you enter the command, the prompt "Type CTRL/D to finish" is displayed on your screen. Enter a banner message of up to 255 characters. Spaces, special characters except "!" and "?", and carriage returns are allowed. When you are finished, hold down the CTRL key and type D.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example creates the banner "Production Switch 1P":

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

This example sets the banner with the default setting:

```
awplus> enable
awplus# configure terminal
awplus(config)# banner exec default
```

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. If the switch also has a message-of-the-day banner, this message is displayed second.

After you enter the command, the prompt “Type CTRL/D to finish” is displayed on your screen. Enter a login message of up to 3,999 alphanumeric characters. Spaces, special characters except “!” and “?,” and carriage returns are allowed. When you are finished, hold down the CTRL key and type D.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

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.
```

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. If the switch also has a login banner, this message is displayed first.

After you enter the command, the prompt "Type CTRL/D to finish" is displayed on your screen. Enter a message-of-the-day banner of up to 255 alphanumeric characters. Spaces, special characters except "!" and "?", and carriage returns are allowed. When you are finished, hold down the CTRL key and type D.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

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

```
awplus> enable
awplus# configure terminal
awplus(config)# banner motd
Type CTRL/D to finish
*** Authorized User Only ***
```

BOOT SYSTEM

Syntax

```
boot system file_name.img
```

Parameter

file_name.img
: Specifies the name of a management software image file that the switch uses when the system is rebooted or reloaded. The file name must have an “img” extension.

Mode

Global Configuration mode

Description

Use this command to specify the name of a management software image file that the switch uses when the system is rebooted or reloaded.

Note
The setting of this command is stored directly in the boot setting that the bootloader uses. You do not need to use the COPY or WRITE command to save this setting.

Example

This example sets the DC2552-1.2.img file as the management software file that will be used when the system is rebooted or reloaded:

```
awplus> enable
awplus# configure terminal
awplus(config)# boot system DC2552-1.2.img
```

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 a 24-hour format. Each value can be in one or two digits. For example, 11:08 PM can be entered either 23:08:00 or 23:8:0.

`dd`

Specifies the day of the month. The day can be in one or two digits. For example, the fourth day of the month can be entered either 4 or 04.

`mmm`

Specifies the month. The month must be specified by its first three letters. This value is not case-sensitive. For example, July is jul and November is nov.

`yyyy`

Specifies the year. The year must be specified in four digits, for example, 2012 and 2013.

Mode

Privileged Exec mode

Confirmation Command

"SHOW CLOCK" on page 105

Description

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

The date and time are set directly in the real-time clock embedded in the switch so that you do not need to save the clock setting using the WRITE or COPY commands. The date and time setting is retained when the switch is reset or powered off.

When the NTP client on the switch is enabled, the NTP server overwrites the date and time set by the CLOCK SET command and you cannot issue the CLOCK SET command on the command line.

Example

This example sets the time and date to 2:15 pm, April 7, 2012:

```
awplus> enable
awplus# clock set 14:15:0 7 Apr 2012
```

ERASE STARTUP-CONFIG

Syntax

```
erase startup-config
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to delete the 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.

Example

This example erases the startup-config file and resets the switch with the default settings:

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

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

HOSTNAME

Syntax

`hostname` *`hostname`*

Parameter

`hostname`

Specifies a name of up to 39 alphanumeric characters for the switch. A host name can contain special characters except spaces, exclamation marks (!), question marks (?), apostrophes (‘), and double quotation marks (“).

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 “awplus.”

When you issue this command, the host name is set to the Management Information Base (MIB)-II “sysName” for SNMP. By default, the sysName has no value.

Example

This example assigns the name “Switch1” to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# hostname Switch1
Switch1(config)#
```

NO BANNER EXEC

Syntax

```
no banner exec
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to delete the banner set with the BANNER EXEC command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example deletes the banner:

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

NO BANNER LOGIN

Syntax

```
no banner login
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to delete the login banner set with the BANNER LOGIN command.

Example

This example removes the login banner:

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

NO BANNER MOTD

Syntax

```
banner motd
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to delete the message-of-the-day banner set with the BANNER MOTD command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

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

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

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. This command also deletes the value of the MIB-II object "sysName."

Example

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

```
Switch_3> enable
Switch_3# configure terminal
Switch_3(config)# no hostname
awplus(config)#
```

REBOOT

Syntax

```
reboot
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to reset the switch. This command is identical to "RELOAD" on page 102.

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.

Note
The switch discards any configuration changes that have not been saved. To save your changes, enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command before resetting the switch. See "WRITE" on page 156 or "COPY RUNNING-CONFIG STARTUP-CONFIG" on page 149.

Example

This example resets the switch:

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

RELOAD

Syntax

```
reload
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to reset the switch. This command is identical to “REBOOT” on page 101.

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.

Note
The switch discards any configuration changes that have not been saved. To save your changes, enter the WRITE command or the COPY RUNNING-CONFIG STARTUP-CONFIG command *before* resetting the switch. See “WRITE” on page 156 or “COPY RUNNING-CONFIG STARTUP-CONFIG” on page 149.

Example

This example resets the switch:

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

SHOW BOOT

Syntax

```
show boot
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the information about the management software and configuration file. See Figure 14 for an example of the output.

```
Current software: ....... DC-2.5.1.1.img
Current boot image: ..... DC-2.5.1.1.img
Default boot config:..... /config/boot.cfg
Current boot config:....../config/boot.cfg (file exists)
```

Figure 14. SHOW BOOT Command

The fields are described in Table 8.

Table 8. SHOW BOOT Command

Field	Description
Current software	Displays the name of the management software file that is currently loaded on the switch.
Current boot image	Displays the name of the management software file that will be loaded when the system is rebooted or reloaded.
Default boot config	Displays the name of the default boot configuration file. It is always "/config/boot.cfg."
Current boot config	Displays the name of the boot configuration file that will be used when the system is rebooted or reloaded.

Example

This example displays the information about the management software and configuration files:

```
awplus# show boot
```

SHOW CLOCK

Syntax

```
show clock
```

Parameters

None

Modes

User Exec and Privilege Exec modes

Description

Use this command to display the system's current date and time. When the NTP client is enabled, this command displays the local time as well as the Coordinated Universal Time (UTC) and the time zone offset.

See Figure 15 for an example of the command output.

```
Local Time; Mon, 2 Jul 2012 14:43:10
UTC Time: Mon, 2 Jul 2012 22:43:10
Timezone Offset; -08:00
```

Figure 15. SHOW CLOCK Command

The fields are described in Table 9.

Table 9. SHOW CLOCK Command

Field	Description
Local Time	Displays the system's current date and time.
UTC Time	Displays the Coordinated Universal Time (UTC) only when the NTP client is enabled.
Timezone Offset	Displays the offset from UTC only when the NTP is enabled.

Example

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

```
awplus> show clock
```

SHOW CPU

Syntax

```
show cpu [sort pri|runtime|sleep|thrds]
```

Parameters

`pri`
Sorts the list by process priorities.

`runtime`
Sorts the list by the runtime of the processes.

`sleep`
Sorts the list by the average sleeping times.

`thrds`
Sorts the list by the number of threads.

Modes

Privilege Exec modes

Description

Use this command to display a list of running processes with their CPU utilization. If you do not specify any of the sorting keywords, the command displays a list of running processes by their process ID numbers.

Figure 16 on page 107 shows an example of the command output.

```
CPU averages:
 1 second: 18% 20 seconds: 100%, 60 seconds: 68%
System load averages:
 1 minute: 1.03, 5 minutes: 1.98, 15 minutes: 1.30

user process
============
  pid  name           thrds   cpu%  pri   state  Sleep%  runtime
 1075  (rcS)              1   0.00   15   sleep    0         105
 1106  (S900ed)           1   0.00   15   sleep    0           0
 1107  (rc.product-end)   1   0.00   15   sleep    0        1094
 1125  (MainTask)         1   0.84   15   sleep    0       12041

Kernel Threads
==============
  pid  name                 cpu%  pri   state  Sleep%  runtime
    1  (init)               0.00   15   sleep    0        1580
    2  (kthreadd)           0.00   15   sleep    0           0
    3  (ksoftirqd/0)        0.00   15   sleep    0           0
    4  (watchdog/0)         0.00   15   sleep    0           0
    5  (events/0)           0.00   15   sleep    0           3
    6  (khelper)            0.00   15   sleep    0           1
    9  (async/mgr)          0.00   15   sleep    0           0
   85  (sync_supers)        0.00   15   sleep    0           0
   87  (bdi_default)        0.00   15   sleep    0           0
```

Figure 16. SHOW CPU Command

The fields are described in Table 10.

Table 10. SHOW CPU Command

Parameter	Description
CPU averages	Displays the average CPU utilizations, in percentages, for the past one second, 20 seconds, and 60 seconds.
System load averages	Displays the average numbers of processes in the wait state for the past one minute, five minutes, and 15 minutes.
User processes / Kernel Threads	Displays information per user process and per Kernel thread.

Table 10. SHOW CPU Command (Continued)

Parameter		Description
	pid	Displays the process ID number.
	name	Displays the name of the program that generated the process.
	thrds	Displays the number of the threads that the process consists of.
	cpu%	Displays the CPU usage of the process.
	pri	Displays the priority level of the process.
	state	Displays the state of the process. The options are: ❒ run ❒ sleep ❒ zombie ❒ dead
	sleep%	Displays the wait state (sleep state) percentage of the process.
	runtime	Displays the runtime of the process in tick. A tick is an interval of the system timer interrupt.

Examples

This example lists the running processes and displays their CPU information:

```
awplus> show cpu
```

This example lists the running processes by runtimes:

```
awplus> show cpu sort runtime
```

SHOW CPU HISTORY

Syntax

```
show cpu history
```

Parameters

None

Modes

Privilege Exec modes

Description

Use this command to display graphs of historical CPU utilization on the switch. See Figure 17 for an example of the command output.

```
Per second CPU load history

100  ************************************************
 90                                                 *
 80
 70
 60
 50
 40
 30                                                  *     *
 20                                                 ** ****
 10
    |....|....|....|....|....|....|....|....|....|....
    oldest                                          Newest
         CPU load% per second (last 60 seconds)
               * = average CPU load%
```

Figure 17. SHOW CPU HISTORY Command

Example

This example displays graphs of historical CPU utilization on the switch:

```
awplus> show cpu history
```

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 amounts of memory the processes are currently using.

`stk`
: Sorts the list by the stack sizes of the processes.

Mode

Privilege Exec mode

Description

Use this command to display the memory consumption of each process. Figure 18 shows an example of the command output.

```
CPU averages:
 1 second: 16% 20 seconds: 18%, 60 seconds: 18%
System load averages:
 1 minute: 0.12, 5 minutes: 0.38, 15 minutes: 0.29
RAM total: 2075652 kB; free: 1871136 kB; buffers: 608 kB

user process
============
  pid  name               mem%    size    peak    data    stk
 1075  (rcS)              0.02    2392    2392     172     84
 1106  (S900ed)           0.02    2388    2388     168     84
 1107  (rc.product-end)   0.02    2388    2388     168     84
 1125  (MainTask)         0.57  422624  438240  412472     84
```

Figure 18. SHOW MEMORY Command

The fields are described in Table 11.

Table 11. SHOW MEMORY Command

Parameter		Description
CPU averages		Displays the average CPU utilizations, in percentages, for the past one second, 20 seconds, and 60 seconds.
System load averages		Displays the average numbers of processes in the wait state for the past one minute, five minutes, and 15 minutes.
RAM total		Displays the total size of RAM.
free		Displays the size of available RAM.
buffers		Displays the size of RAM that is assigned to Kernel buffers.
user processes		Displays information per user process.
	pid	Displays the process ID number.
	name	Displays the name of the program that generated the process.
	mem%	Displays the RAM usage by the process.
	size	Displays the amount of memory that the process is currently using.
	peak	Displays the peak amount of memory that the process has ever used.
	data	Displays the amount of memory that the process is currently using for data.
	stk	Displays the amount of memory that the process is currently using for stacking.

Examples

This example displays the memory consumptions of the processes sorted by process ID numbers:

```
awplus> show memory
```

This example displays the memory consumptions sorted by size:

```
awplus> show memory sort size
```

SHOW MEMORY HISTORY

Syntax

```
show memory history
```

Parameters

None

Modes

Privilege Exec modes

Description

Use this command to display graphs of historical memory utilization. See Figure 19 for an example of the command output.

```
Per second memory utilization history

100
 90
 80
 70
 60
 50
 40
 30
 20
 10  ************************************************
     |....|....|....|....|....|....|....|....|....|....
     oldest                                        Newest
          Memory utilization% per second (last 60 seconds)
                * = average memory load%
```

Figure 19. SHOW MEMORY HISTORY Command

Example

This example displays graphs of historical memory utilization:

```
awplus> show memory history
```

SHOW PROCESS

Syntax

```
show process [sort cpu|mem]
```

Parameters

`cpu`
: Sorts the list by the CPU usage of the processes.

`mem`
: Sorts the list by the amounts of memory the processes are currently using.

Mode

Privilege Exec mode

Description

Use this command to display a list of running processes with their CPU utilization. Without specifying any sorting keywords, the command displays a list of running processes by process ID numbers.

See Figure 20 on page 114 for an example of the command output.

```
CPU averages:
 1 second: 23% 20 seconds: 36%, 60 seconds: 32%
System load averages:
 1 minute: 0.28, 5 minutes: 1.44, 15 minutes: 1.17

user process
============
  pid  name           thrds   cpu%  mem%    pri   state  sleep%
 1075  (rcS)              1   0.00  0.02     15   sleep   0
 1106  (S900ed)           1   0.00  0.02     15   sleep   0
 1107  (rc.product-end)   1   0.00  0.02     15   sleep   0
 1125  (MainTask)         1   1.68  0.60     15   sleep   0

Kernel Threads
==============
  pid  name                   cpu%   pri  state   Sleep%
    1  (init)                 0.00    15  sleep     0
    2  (kthreadd)             0.00    15  sleep     0
    3  (ksoftirqd/0)          0.00    15  sleep     0
    4  (watchdog/0)           0.00    15  sleep     0
    5  (events/0)             0.00    15  sleep     0
    6  (khelper)              0.00    15  sleep     0
    9  (async/mgr)            0.00    15  sleep     0
   85  (sync_supers)          0.00    15  sleep     0
   87  (bdi_default)          0.00    15  sleep     0
```

Figure 20. SHOW PROCESS Command

The fields are described in Table 12.

Table 12. SHOW PROCESS Command

Field	Description
CPU averages	Displays the average CPU utilizations, in percentages, for the past one second, 20 seconds, and 60 seconds.
System load averages	Displays the average numbers of processes in the wait state for the past one minute, five minutes, and 15 minutes.
User processes / Kernel Threads	Displays information per user process.

Table 12. SHOW PROCESS Command (Continued)

Field		Description
	pid	Displays the process ID number.
	name	Displays the name of the program that generated the process.
	thrds	Displays the number of the threads that the process consists of.
	cpu%	Displays the CPU usage of the process.
	mem%	Displays the RAM usage of the process.
	pri	Displays the priority level of the process.
	state	Displays the state of the process. The options are: ❒ run ❒ sleep ❒ zombie ❒ dead
	sleep%	Displays the wait state (sleep state) percentage of the process.

Examples

This example lists the running processes by process ID numbers:

```
awplus> show process
```

This example lists the running processes by CPU utilization:

```
awplus> show process sort cpu
```

SHOW RUNNING-CONFIG

Syntax

```
show running-config [snmp|log]
```

Parameters

`snmp`
: Specifies the only SNMP section of the running-config file is displayed.

`log`
: Specifies the only LOG section of the running-config file is displayed.

Modes

Privileged Exec mode

Description

Use this command to display the current settings of the switch. The current settings of the switch are called the running-config and these are stored in RAM. The command displays the settings that have been changed from their default values and include the settings that have not yet been saved in the startup-config file. Parameters that retain their default settings are not included in the running-config file.

When entered with the SNMP or LOG keyword, the command displays the only SNMP section or the only LOG section of the running-config file, respectively. Without specifying a keyword, the command displays all of the contents of the running-config file.

Example

This example displays the current settings of the switch:

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

SHOW SWITCH

Syntax

```
show switch
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display information about the switch as shown in Figure 21.

```
Switch Information:
Application Software Version ......... 2.5.1.1
Application Software Build date ...... Oct 31 2011 10:24:12
MAC Address ........................... 00:E0:0C:02:10:FD
Active Spanning Tree version ......... RSTP
Console Disconnect Timer Interval .... 10 minute(s)
Telnet Server status .................. Enabled
MAC address aging time ................ 300 second(s)
Multicast Mode ....................... Unknown
```

Figure 21. SHOW SWITCH Command

The fields are described in Table 13.

Table 13. SHOW SWITCH Command

Field	Description
Application Software Version	Indicates the version number of the management software.
Application Software Build Date	Indicates the date and time the management software was built.
MAC Address	Indicates the MAC address of the switch.
Active Spanning Tree Version	Indicates the name of the active spanning tree protocol as STP, RSTP, or MSTP.

Table 13. SHOW SWITCH Command (Continued)

Field	Description
Console Disconnect Timer Interval	Indicates the current setting of the console timer. The switch ends management sessions if no management activity is performed for the length of the timer.
Telnet Server Status	Indicates the status of the Telnet server. You can manage the switch remotely from a Telnet client on your network when the server is enabled. When the server is disabled, the switch cannot be managed remotely with a Telnet client.
MAC Address Aging Time	Indicates the current setting of the aging timer, which the switch uses to delete inactive dynamic MAC addresses from the MAC address table.

Example

This example displays information about the switch:

```
awplus# show switch
```

SHOW SYSTEM

Syntax

```
show system
```

Parameters

None

Modes

User Exec mode

Description

Use this command to display general information about the switch. See Figure 22 for an example of the information.

```
Switch System Status              Sat, 01 Jan 2012 00:37:26

Board        Bay     Board Name     Rev        Serial Number
-------------------------------------------------------------------
Base         PSU1    AT-DC2552XS    R1         S05525A023600001
PSU          PSU2    AT-PWR06       A1         07865R110200002
PSU          PSU2    AT-PWR06       A1          07865R110200001
Fan Module   FAN1    FAN Tray 01
Fan Module   FAN2    FAN Tray 02
-------------------------------------------------------------------

Environmental Status     : Normal
Uptime                   : 0 days 00:37:27
Bootloader version       : U-Boot 2009.11 - ver1.0.0
Bootloader build date    : Oct 31 2011 15:55:28

Current software         : DC-2.5.1.1.img
Software Version         : 2.5.1.1
Build date               : Oct 31 2011 15:40:44

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

System Name              : myswitch

System Contact           : neadmin@alliedtelesis.com

System Location          : 5FUPD3
```

Figure 22. SHOW SYSTEM Command

The fields are described in Table 14.

Table 14. SHOW SYSTEM Command

Field	Description
Date and time	Indicates the setting of the system clock.
Board	Indicates a component. The components are: ❒ Base- Indicates the switch. ❒ PSU - Indicates the Power supply unit. ❒ Fan module - Indicates the fan module.
Bay	Indicates a slot number for the board (component). The base (switch) does not have a slot number.
Board Name	Indicates the name of the board.
Revision	Indicates the hardware revision number of the board.
Serial Number	Indicates the serial number of the board.
Environment Status	Indicates the status of the switch. The options are: ❒ Normal ❒ "***Fault*** To view more detailed information, use the SHOW SYSTEM ENVIRONMENT command. See "SHOW SYSTEM ENVIRONMENT" on page 122.
Uptime	Indicates the length of time since the switch was last reset or power cycled.
Bootloader version	Indicates the version of the bootloader.
Bootloader build date	Indicates the date and time the bootloader was built.
Current software	Indicates the file name of the current management software.
Software version	Indicates the version number of the current management software.
Build date	Indicates the date and time the current management software was built.

Table 14. SHOW SYSTEM Command (Continued)

Field	Description
Current boot config	Indicates the name of the configuration file used by the switch when the switch is reset or power cycled. The configuration file that is used by the switch when the switch is reset or power cycled is called a startup-config file.
Territory	N/A
System name	Indicates the name of the system set in the sysName in the Management Information Base (MIB)-II.
System contact	Indicates the contact information for the system set in the sysContact in the MIB-II.
System Location	Indicates the location of the system set in the sysLocation in the MIB-II.

Example

This example displays information about switch:

```
awplus# show system
```

SHOW SYSTEM ENVIRONMENT

Syntax

```
show system environment
```

Parameters

None

Mode

Privilege Exec mode

Description

Use this command to display information about the switch, PSUs, and fan modules. See Figure 23 for an example of this information.

```
Environment Monitoring Status
Overall Status: Normal

Resource ID: 01 Name: AT-DC2552XS

ID  Sensor (Units)                Reading    Low Limit  High Limit  Status
1   VCC3V3                            Yes     -          -              OK
2   MAC1V                             Yes     -          -              OK
3   DDRvV5                            Yes     -          -              OK
4   PHY1VL                            Yes     -          -              OK
5   PHY1VR                            Yes     -          -              OK
6   Temp: Near CPU (Degrees C)         33     -          -              Ok
7   Temp: Near MAC (Degrees C)         45     -          -              Ok
8   Temp: PHY left (Degrees C)         49     -          -              Ok
9   Temp: PHY right (Degrees C)        45     -          -              Ok

Resource ID: 02 Name: AT-DC2552XS

ID  Sensor (Units)                Reading    Low Limit High Limit   Status
1   Device Present                    Yes     -          -              Ok
2   PSU Connection                    Yes     -          -              Ok
3   PSU Overtemp                      Yes     -          -              Ok
4   PSU Fan Fail                      Yes     -          -              Ok
```

Figure 23. SHOW SYSTEM ENVIRONMENT Command

The fields are described in Table 15.

Table 15. SHOW SYSTEM ENVIRONMENT Command

Field	Description
Overall Status	Indicates the status of the unit. The status is either "Normal" or "***Fault***."
Resource ID	Indicates the ID of the module.
Name	Indicates the name of the module. The module names are: ❒ AT-DC2552XS- Indicates the switch. ❒ AT-PWR06 - Indicates the power supply unit. ❒ FAN Tray 01 or 02 - Indicates a fan module.
ID	Indicates the ID of the sensor.
Sensor (Units)	Indicates the name of the sensor.
Reading	Shows the value that the sensor detected.
Low Limit	Displays the specified maximum temperature. When no value is set, "-" is displayed.
High Limit	Displays the specified minimum temperature. When no value is set, "-" is displayed.
Status	Indicates the status of the sensor. The options are: ❒ Ok ❒ fault

Example

This example displays information about the switch, PSUs, and fan modules:

```
awplus# show system environment
```

SHOW SYSTEM PLUGGABLE

Syntax

```
show system pluggable
```

Parameters

None

Mode

User Exec mode

Description

Use this command to display information about the SFP+ and QSFP+ modules in the switch. See Figure 24 for an example of the output. The SHOW SYSTEM PLUGGABLE DETAIL command provides more detailed information about the SFP+ and QSFP+ modules. See “SHOW SYSTEM PLUGGABLE DETAIL” on page 126.

```
System Pluggable Information
Port    Vendor   Device       Serial Number     Datecode     Type
-------------------------------------------------------------------------
1.0.1   ATI      ATI-SP10SR   A04440R11140001   20110330     10GBASE-SR
1.0.2   ATI      ATI-SP10SR   A04440R111400028  20110330     10GBASE-SR
-------------------------------------------------------------------------
```

Figure 24. SHOW SYSTEM PLUGGABLE Command

The fields are described in Table 16.

Table 16. SHOW SYSTEM PLUGGABLE Command

Field	Description
Port	Indicates the port ID.
Vendor	Indicates the vendor of the SFP+/QSFP+ module.
Device	Indicates the product name of the SFP+/QSFP+ module.
Serial Number	Indicates the serial number of the SFP+/QSFP+ module.

Table 16. SHOW SYSTEM PLUGGABLE Command (Continued)

Field	Description
Datecode	Indicates the date the SFP+/QSFP+ module was produced.
Type	Indicates the cable specification for the SFP+/ QSFP+ module. The types are: ❒ 10GBASE-SR (AT-SP10SR) ❒ 10GBASE-LR (AT-SP10LR) ❒ 1xCOPPER PAS (AT-SP10TW1/3/7) ❒ 40GBASE-SR (AT-QSFPSR) ❒ 4xCOPPER PAS (AT-QSFP1CU/3CU)

Example

This example displays information about the SFP+ and QSFP+ modules:

```
awplus> show system pluggable
```

SHOW SYSTEM PLUGGABLE DETAIL

Syntax

```
show system pluggable detail
```

Parameters

None

Mode

User Exec mode

Description

Use this command to display information about the SFP+ and QSFP+ modules in the switch. See Figure 25 for an example of the output.

```
Port1.0.1
==========
Vendor Name:                    ATI
Device Name:                    AT-SP10SR
Device Type:                    10GBASE-SR
Serial Number:                  A04440R111400010
Manufacturing Detecode:         20110330
SFP Laser Wavelength:           850nm
Link Length Supported
  OM1 (62.5um) Fiber:           30m
  OM2 (50um) Fiber:             80m
  OM3 (50um) Fiber:             300m

Port1.0.2
==========
Vendor Name:                    ATI
Device Name:                    AT-SP10SR
Device Type:                    10GBASE-SR
Serial Number:                  A04440R111400028
Manufacturing Detecode:         20110330
SFP Laser Wavelength:           850nm
Link Length Supported
  OM1 (62.5um) Fiber:           30m
  OM2 (50um) Fiber:             80m
  OM3 (50um) Fiber:             300m
.....
```

Figure 25. SHOW SYSTEM PLUGGABLE DETAIL Command

The fields are described in Table 17.

Table 17. SHOW SYSTEM PLUGGABLE DETAIL Command

Field		Description
Port		Indicates the port ID.
Vendor Name		Indicates the vendor of the SFP+/QSFP+ module.
Device Name		Indicates the product name of the SFP+/ QSFP+ module.
Device Type		Indicates the cable specification of the SFP+/ QSFP+ module. The types are: ❒ 10GBASE-SR (AT-SP10SR) ❒ 10GBASE-LR (AT-SP10LR) ❒ 1xCOPPER PAS (AT-SP10TW1/3/7) ❒ 40GBASE-SR (AT-QSFPSR) ❒ 4xCOPPER PAS (AT-QSFP1CU/3CU)
Serial Number		Indicates the serial number of the SFP+/ QSFP+ module.
Manufacturing Datecode		Indicates the date the SFP+/QSFP+ module was produced.
SFP Laser Wavelength		Indicates the laser wavelength of the SFP+/ QSFP+ module.
	OM1 (62.5 µm) Fiber	Indicates the maximum distance of 62.5/125 µm multimode optic fiber (OM1) cable supported by the SFP+/QSFP+ module.
	OM2 (50 µm) Fiber	Indicates the maximum distance of 50/125 µm multimode optic fiber (OM2) cable supported by the SFP+/QSFP+ module.
	OM3 (50 µm) Fiber	Indicates the maximum distance of 50/125 µm multi-mode optic fiber (OM3) cable supported by the SFP+/QSFP+ module.

Example

This example displays detailed information about the SFP+ and QSFP+ module modules:

```
awplus> show system pluggable detail
```

SHOW SYSTEM SERIALNUMBER

Syntax

```
show system serialnumber
```

Parameters

None

Mode

User Exec mode

Description

Use this command to display the serial number of the switch. The serial number is also displayed with the SHOW SYSTEM command. See “SHOW SYSTEM” on page 119.

Example

This example displays the serial number of the switch:

```
awplus> show system serialnumber
```

SHOW TECH-SUPPORT

Syntax

```
show tech-support [all]
```

Parameter

`all`
: Includes all debug messages in the debug log file.

Mode

Privilege Exec

Description

Use this command to generate a debug log file for troubleshooting. Without the all keyword, this command lists the selected debug messages in the debug log file. Contact Allied Telesis technical support when you use the debug messages. See Figure 26 for an example of the command execution.

```
Generating output to /config/tech-support-20351031012059.txt: ...... done.
```

Figure 26. SHOW TECH-SUPPORT Command

Example

This example generates a debug log file:

```
awplus# show tech-support
```

SHOW VERSION

Syntax

```
show version
```

Parameters

None

Mode

User Exec mode

Description

Use this command to display the software version number and build date of the management software. See Figure 27 for an example of the information.

```
AlliedWare plus (TM) 2.5.1.1 00/31/11 15:40:44

Build name             : DC-2.5.1.1.img
Build date             : Oct 31 2011 15:40:44
Build type             : RELEASE

Bootloader version     : U-Boot 2009.11 - ver1.0.0
Bootloader build date  : Oct 31 2011 15:55:28
```

Figure 27. SHOW VERSION Command

The fields are described in Table 18.

Table 18. SHOW VERSION Command

Field	Description
AlliedWare Plus (TM)	Indicates the version number of the management software and the date and time it was built.
Build name	Indicates the name of the management software image file.
Build date	Indicates the build date and time the management software was built.
Build type	Indicates the type of the management software.

Table 18. SHOW VERSION Command (Continued)

Field	Description
Bootloader version	Indicates the version of the bootloader.
Bootloader build date	Indicates the date and time the bootloader was built.

Example

This example displays the version numbers and build dates of the management software and bootloader:

```
awplus# show version
```

Chapter 5

File Management Commands

The file management commands are summarized in Table 19.

Table 19. File Management Commands

Command	Mode	Description
“COPY” on page 134	Privileged Exec	Copies a boot configuration file in the Flash memory on the switch.
“COPY FLASH TFTP” on page 135	Privileged Exec	Uses TFTP to upload a file from the switch.
“COPY HTTP FLASH” on page 136	Privileged Exec	Uses HTTP to download a file to the switch.
“COPY TFTP FLASH” on page 137	Privileged Exec	Uses TFTP to download a file to the switch.
“COPY ZMODEM” on page 138	Privileged Exec	Uses Zmodem to download and upload a file from the Console terminal.
“DELETE” on page 139	Privileged Exec	Deletes a file from the file system in the switch.
“DIR” on page 140	Privileged Exec	Lists the names of the files stored in the file system on the switch.
“MOVE” on page 141	Privileged Exec	Renames files in the switch’s file system.
“SHOW FILE” on page 142	Privileged Exec	Displays the contents of a file in the file system in the switch.
“SHOW FILE SYSTEMS” on page 143	Privileged Exec	Displays the specifications of the file system in the switch.

COPY

Syntax

`copy` *`sourcefile`*`.cfg` *`destinationfile`*`.cfg`

Parameters

`sourcefile``.cfg`
Specifies the name of a configuration file you want to copy.

`destinationfile``.cfg`
Specifies the name of the new copy of the file. The destination filename can be from 1 to 28 alphanumeric characters. It is case-sensitive. The extension must be ".cfg." Spaces and special characters are *not* allowed.

Mode

Privileged Exec mode

Description

Use this command to copy a configuration file in the Flash memory on the switch. If the destination filename has the same name as an existing file, the command overwrites the existing file.

Confirmation Command

"DIR" on page 140

Examples

This command copies the configuration file "test1.cfg" and saves as "test1backup.cfg":

```
awplus# copy test1.cfg test1backup.cfg
```

COPY FLASH TFTP

Syntax

```
copy flash tftp ipaddress filename
```

Parameters

ipaddress
: Specifies the IPv4 address of a TFTP server on your network.

filename
: Specifies the filename of a file to upload from the file system in the switch to a TFTP server. The file extension can be "cfg" or "txt." You cannot specify a configuration file, which has the extension "img."

Mode

Privileged Exec mode

Description

Use this command to upload a file from the file system in the switch to a TFTP server on your network.

Before issuing this command, the switch must have a management IPv4 address assigned. See "IP ADDRESS" on page 404 and "IP ADDRESS DHCP" on page 406.

Example

This command uploads the configuration file "test1.cfg" from the file system in the switch to a TFTP server that has the IP address 192.168.1.200:

```
awplus> enable
awplus# copy flash tftp 192.168.1.200 test1.cfg
```

COPY HTTP FLASH

Syntax

```
copy http flash ipaddress filename
```

Parameters

ipaddress
: Specifies the IPv4 address of a HTTP server on your network.

filename
: Specifies a file on the HTTP server to download to the switch. The file extensions must be “bin,” “cfg,” “img,” “inf,” “ldr,” “sys,” “tmp,” “txt,” “ukf,” “key,” “cer,” “csr,” “log,” or “tgz.” The filename *cannot* contain spaces.

Mode

Privileged Exec mode

Description

Use this command to download a file to the switch from a HTTP server on you network. The file to download must be placed in the root directory of the HTTP server.

Before issuing this command, the switch must have a management IPv4 address assigned. See “IP ADDRESS” on page 404 and “IP ADDRESS DHCP” on page 406.

Confirmation Command

“DIR” on page 140

Examples

This command downloads the new management software file “dc-2.5.1.2.img” to the switch from a HTTP server with an IP address of 192.168.1.70:

```
awplus> enable
awplus# copy tftp flash 192.168.1.70 dc-2.5.1.2.img
```

This command downloads the configuration file “test2.cfg” to the switch from a HTTP server with an IP address of 192.168.1.70:

```
awplus> enable
awplus# copy tftp flash 192.168.1.70 test2.cfg
```

COPY TFTP FLASH

Syntax

```
copy tftp flash ipaddress filename
```

Parameters

ipaddress
: Specifies the IPv4 address of a TFTP server on your network.

filename
: Specifies a file on the TFTP server to download to the switch. The file extensions must be "bin," "cfg," "img," "inf," "ldr," "sys," "tmp," "txt," "ukf," "key," "cer," "csr," "log," or "tgz." The filename *cannot* contain spaces.

Mode

Privileged Exec mode

Description

Use this command to download a file to the switch from a TFTP server on you network.

Before issuing this command, the switch must have a management IPv4 address assigned. See "IP ADDRESS" on page 404 and "IP ADDRESS DHCP" on page 406.

Confirmation Command

"DIR" on page 140

Examples

This command uploads the new management software file "dc-2.5.1.2.img" to the switch from a TFTP server with an IP address of 192.168.1.70:

```
awplus> enable
awplus# copy tftp flash 192.168.1.70 dc-2.5.1.2.img
```

This command downloads the configuration file "test2.cfg" to the switch from a TFTP server with an IP address of 192.168.1.70:

```
awplus> enable
awplus# copy tftp flash 192.168.1.70 test2.cfg
```

COPY ZMODEM

Syntax

```
copy [filename] zmodem
```

Parameter

filename
: Specifies the name of a file you want to upload. You cannot specify a file with the file extension “img.”

Mode

Privileged Exec mode

Description

Use this command together with a Zmodem utility to upload a file in the switch to the terminal or management workstation and download a file on the terminal or management workstation to the file system in the switch. You must use a Console terminal that support a Zmodem utility to use this command.

To upload a file on the file system in the switch to the terminal or management workstation, specify the *filename* parameter. You are not allowed to upload a file with the file extension “img” using a Zmodem utility.

To download a file in the terminal or management workstation to the switch, you must specify a file using a Zmodem utility. The switch accepts the file extensions: “bin,” “cfg,” “img,” “inf,” “ldr,” “sys,” “tmp,” “txt,” “ukf,” “key,” “cer,” “csr,” “log,” or “tgz.”

Examples

This command uploads the configuration file “test.cfg” on the file system in the switch to the terminal or management workstation:

```
awplus# copy test.cfg zmodem
```

This command downloads the configuration file “test2.cfg” by an operation on the Zmodem utility on the terminal or the management workstation:

```
awplus# copy zmodem
```

DELETE

Syntax

```
delete [force] filename
```

Parameters

`force`
: Specifies the command does not display the confirmation prompt, "Delete *filename*? (y/n)," after you enter the command. To display the confirmation prompt, do not include this option.

`filename`
: Specifies the filename to delete from the file system on the switch. To delete multiple configuration files, use the wildcard "*" to replace any part of a filename.

Mode

Privileged Exec mode

Description

Use this command to delete a file from the file system on the switch.

Confirmation Command

"DIR" on page 140

Examples

This command deletes the configuration file "unit12.cfg":

```
awplus# delete unit12.cfg
```

This command deletes all configuration files that start with "bl":

```
awplus# delete bl*.cfg
```

This command deletes all text files for troubleshooting without asking you for confirmation:

```
awplus# delete force tech-support-*.txt
```

DIR

Syntax

```
dir
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to list the names of the files stored in the file system on the switch.

Figure 28 is an example of the information.

```
15889581  -rw-r--r-- Nov 7 2011 10:42:05 DC-2.5.1.1.img
    457  -rw-r--r-- Nov 19 2011 10:24:08 b.cfg
    527  -rw------- Nov 19 2011 00:03:33 ssh_host_key
    331  -rw------- Nov 19 2011 00:03:33 ssh_host_key.pub
    457  -rw-r--r-- Nov 20 2011 10:24:08 a.cfg
 270807  -rw-r--r-- Oct 12 2011 00:00:43 EventPermanentLog.txt
    367  -rw------- Oct 19 2011 00:15:30 boot.cfg
      0  -rw-r--r-- Oct 24 2011 00:03:33 WarmBootFile
```

Figure 28. DIR Command

Example

This example lists the names of the files stored in the file system:

```
awplus# dir
```

MOVE

Syntax

```
move source_filename destination_filename
```

Parameters

source_filename
: Specifies the name of a file to be renamed. The filename is case-sensitive.

destination_filename
: Specifies the new name for the file. The filename is case-sensitive and can be from 1 to 32 alphanumeric characters including the filename extension. The filename cannot contain spaces or special characters.

Mode

Privileged Exec mode

Confirmation Command

"DIR" on page 140

Description

Use this command to rename files in the switch's file system. If you specify the name of an existing file for the destination file, the new file overwrites the existing file.

Example

This example renames the file "sw1.cfg" to "swrm102.cfg":

```
awplus# move sw12.cfg swrm102.cfg
```

SHOW FILE

Syntax

```
show file filename
```

Parameter

filename
: Specifies the name of a file in the file system in the switch to display its contents.

Mode

Privileged Exec mode

Description

Use this command to display the contents of the file. If the file contains characters other than ASCII characters (0x00 to 0x7f), the characters are not displayed properly.

Example

This example displays the contents of the file “boot.cfg”:

```
awplus# show file boot.cfg
```

SHOW FILE SYSTEMS

Syntax

```
show file systems
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the specifications of the file system on the switch. An example is shown in Figure 29.

```
Size(b)   Free(b)   Type    Flags    Prefixes    S/D/V    Lcl/Ntwk  Avail
-------------------------------------------------------------------------
100.0M    68.1      flash     rw     flash:      static   local     Y
```

Figure 29. SHOW FILE SYSTEMS Command

The fields are described in Table 20.

Table 20. SHOW FILE SYSTEMS Command

Field	Description
Size (B)	Indicates the total memory size of the file system on the switch. The amount is given in bytes.
Free (B)	Indicates the amount of unused file system memory on the switch. The amount is given in bytes.
Type	Indicates the type of memory.
Flags	Indicates the file setting options. The options are: ❒ rw: read and write ❒ ro: read only
Prefixes	Not supported
S/D/V	Indicates the memory type. The switch's memory type is static.

Table 20. SHOW FILE SYSTEMS Command (Continued)

Field	Description
Lcl/Ntwk	Indicates either a local file system or a remote file system. The switch's file system is local.
Y/N	Whether the local file system is accessible. It always displays "Y," which means yes.

Example

This example displays the specifications of the file system on the switch:

```
awplus# show file systems
```

Chapter 6

Boot Configuration File Commands

The boot configuration file commands are summarized in Table 21.

Table 21. Boot Configuration File Commands

Command	Mode	Description
“BOOT CONFIG-FILE” on page 146	Global Configuration	Designates or creates a new boot configuration file (startup-config file) for the switch.
“COPY RUNNING-CONFIG” on page 148	Privileged Exec	Creates a new boot configuration file that contains the current settings of the switch.
“COPY RUNNING-CONFIG STARTUP-CONFIG” on page 149	Privileged Exec	Saves the switch’s current configuration (running-config file) to the boot configuration file (startup-config file).
“COPY STARTUP-CONFIG” on page 15088	Privileged Exec	Saves a configuration file in the switch as the startup configuration file.
“ERASE STARTUP-CONFIG” on page 151	Privileged Exec	Deletes the boot configuration file (startup-config file) and returns the switch to its default settings.
“NO BOOT CONFIG-FILE” on page 152	Global Configuration	Designates the default BOOT.CFG file as the boot configuration file on the switch.
“SHOW BOOT” on page 153	Privileged Exec	Displays the names of the boot configuration file and the configuration file that was used by the switch during the last reset or power cycle.
“SHOW STARTUP-CONFIG” on page 155	Privileged Exec	Displays the contents of the boot configuration file (startup-config file).
“WRITE” on page 156	Privileged Exec	Saves the switch’s current configuration to the boot configuration file (startup-config file).

BOOT CONFIG-FILE

Syntax

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

Parameter

`filename``.cfg`

Specifies the name of a configuration file as the boot configuration file (startup-config file) on the switch. The filename is case-sensitive and can be from 1 to 28 alphanumeric characters. The extension must be ".cfg."

Mode

Global Configuration mode

Description

Use this command to designate the boot configuration file (startup-config file) on the switch. The switch uses the boot configuration file designated by this command when the switch is power-cycled or reset. By default, the boot.cfg file is the boot configuration file. To configure the switch with the new boot configuration file, reset the switch with the REBOOT or RELOAD command after entering this command.

When you issue the WRITE or COPY RUNNING-CONFIG STARTUP-CONFIG command, the switch saves the current configuration settings onto the boot configuration file designated by the BOOT CONFIG-FILE command. In addition, when you issue the ERASE STARTUP-CONFIG command, the switch deletes the boot configuration file designated by the BOOT CONFIG-FILE command. See "ERASE STARTUP-CONFIG" on page 151.

To create a new boot configuration file, enter a new filename in the command. The command automatically creates the new file, updates it with the current settings of the switch, and designates it as the boot configuration file.

Confirmation Command

"SHOW BOOT" on page 153.

Example

This example designates a file called "boot2.cfg" as the switch's boot configuration file:

```
awplus> enable
awplus# configure terminal
awplus(config)# boot config-file boot2.cfg
```

COPY RUNNING-CONFIG

Syntax

```
copy running-config filename..cfg
```

Parameter

filename.cfg
: Specifies a name for the configuration file. The file name is case-sensitive and can be from 1 to 28 alphanumeric characters. The extension must be ".cfg."

Mode

Privileged Exec mode

Description

Use this command to create a new configuration file. The new configuration file is stored in the file system on the switch, containing the current settings of the switch. Use this command to create a backup copy of the switch's current configuration (running-config file).

This command does not change the boot configuration file. To designate a different file as the boot configuration file on the switch, refer to "BOOT CONFIG-FILE" on page 146.

Confirmation Command

"DIR" on page 140

Example

This example saves the current configuration settings of the switch as a new boot configuration file called "sw3_backup.cfg":

```
awplus> enable
awplus# copy running-config sw3_backup.cfg
```

COPY RUNNING-CONFIG STARTUP-CONFIG

Syntax

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

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to save the switch's current configuration file (running-config file) onto the boot configuration file (startup-config file). When you enter the command, the switch copies the current parameter settings in the RAM memory into the boot configuration file in the FLASH memory.

This command is equivalent to "WRITE" on page 156.

Note
Parameter changes in the current management session that are not saved by this command or the WRITE command are discarded when you power off or reset the switch.

Example

This example saves the switch's current configuration settings onto the boot configuration file (startup-config file):

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

COPY STARTUP-CONFIG

Syntax

`copy` *`filename`*`..cfg startup-config`

Parameter

`filename``..cfg`

Specifies the name of a configuration file in the file system in the switch. The file name is case-sensitive. The extension must be ".cfg."

Mode

Privileged Exec mode

Description

Use this command to save a configuration file in the file system in the switch as the startup configuration file.

Confirmation Command

"DIR" on page 140

Example

This example saves a configuration file named "sw2_10_12.cfg" as the startup configuration file:

```
awplus> enable
awplus# copy sw2_10_12.cfg startup-config
```

ERASE STARTUP-CONFIG

Syntax

```
erase startup-config
```

Parameters

None

Mode

Privileged Exec mode

Confirmation Command

"DIR" on page 140

Description

Use this command to delete the startup configuration file, which is specified as the boot configuration file. After entering this command, enter the REBOOT command to reset the switch. The switch restores the default configuration settings.

To resume managing the switch after restoring the default settings, you must establish a local management session from the Console port.

Example

This example deletes the startup configuration file:

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

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

NO BOOT CONFIG-FILE

Syntax

```
no boot config-file
```

Parameter

None

Mode

Global Configuration mode

Description

Use this command to designate the default boot.cfg file as the boot configuration file (startup-config file). The switch is configured with the default settings after you reboot or reset it.

Example

This example sets the startup configuration file to the default settings:

```
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 names of the management software and boot configuration file. See Figure 30 for an example of the command output.

```
Current software     : DC-2.5.1.1.img
Current boot image   : DC-2.5.1.1.img
Default boot config  : /config/boot.cfg
Current boot config  : /config/boot.cfg (file exists)
```

Figure 30. SHOW BOOT Command

The fields are described in Figure 22.

Table 22. SHOW BOOT Command

Field	Description
Current software	Displays the file name of the management software that is currently loaded on the switch.
Current boot image	Displays the file name of the management software that is loaded on the switch next time the switch reboots.
Default boot config	Displays the name of the default boot configuration file. Always displays "/config/boot.cfg." When the BOOT-CONFIG-FILE command has never issued on the switch, the switch uses this file to configure itself when rebooting.

Table 22. SHOW BOOT Command (Continued)

Field	Description
Current boot config	Displays the name of the boot configuration file (startup configuration file) currently specified on the switch. The switch uses this file to configure itself next time the switch reboots.

Example

This example displays the names of the management software and boot configuration file:

```
awplus# show boot
```

SHOW STARTUP-CONFIG

Syntax

```
show startup-config
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the contents of the boot configuration file. The boot configuration file is the startup configuration file that the switch uses to configure itself when the switch is power-cycled or reset. The startup configuration file is the file that you specify with the BOOT CONFIG-FILE command. By default, the startup configuration file is the boot.cfg file. See Figure 31 for an example of this file.

```
!
service maxmanager 3
baud-rate set 115200
...
mac address-table ageing-time 300
!
service password-encryption
!

username manager privilege 15 password 8 3af00c6cad11f7ab5db4467b66ce503e
!
!
endawplus#
```

Figure 31. SHOW START-UP CONFIG Command

Example

This example display the contents of the boot configuration file:

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

WRITE

Syntax

```
write
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to save the configuration file (running-config file) stored on the RAM as the startup-config file stored on the NVRAM on the switch.

This command is equivalent to the COPY RUNNING-CONFIG STARTUP-CONFIG, WRITE MEMORY, or WRITE FILE command.

Confirmation Command

“SHOW STARTUP-CONFIG” on page 155

Example

This example saves the running configuration file:

```
awplus# write
```

Chapter 7

Event Log Commands

The event log commands are summarized in Table 23.

Table 23. Event Log Commands

Command	Mode	Description
“CLEAR LOG” on page 158	Privileged Exec	Deletes entries in the buffered or permanent log.
“DEFAULT LOG” on page 159	Global Configuration	Sets the specified log to default settings.
“LOG” on page 161	Global Configuration	Starts logging event messages to the specified destination.
“LOG (FILTER)” on page 162	Global Configuration	Specifies filtering criteria to the specified destination.
“LOG HOST TIME” on page 165	Global Configuration	Specifies the time for event messages stored in a syslog server.
“LOG SIZE” on page 167	Global Configuration	Specifies the maximum size of memory, in Kbytes, that the switch stores event messages.
“NO LOG” on page 168	Global Configuration	Stops sending event messages to the specified destination.
“SHOW LOG” on page 170	Privileged Exec	Displays the event messages in the buffered log.
“SHOW LOG CONFIG” on page 172	Privileged Exec	Displays the configuration of event logs.
“SHOW LOG PERMANENT” on page 175	Privileged Exec	Displays the event messages in the permanent log.
“TERMINAL MONITOR” on page 177	Privileged Exec	Displays event messages on the console terminal.

CLEAR LOG

Syntax

```
clear log [buffered|permanent]
```

Parameters

`buffered`
: Deletes the event messages in runtime memory (RAM).

`permanent`
: Deletes the event messages stored in the Flash memory.

Mode

Privileged Exec mode

Description

Use this command to delete the event messages in the event log.

Confirmation Command

“SHOW LOG” on page 170

Example

This example deletes the event messages in RAM:

```
awplus# clear log buffered
```

DEFAULT LOG

Syntax

```
default log buffered|permanent|monitor|console|
host ipv4_address
```

Parameters

`buffered`
: Sets the buffered log to the default settings. By default, the maximum memory size is 50 Kbytes, the filtering condition level is informational, and logging in the buffered log is enabled.

`permanent`
: Sets the permanent log to the default settings. By default, the maximum memory size is 50 Kbytes, the filtering condition level is warning, and logging in the permanent log is enabled.

`monitor`
: Sets the terminal monitor output to the default settings. By default, the filtering condition level is debugging.

`console`
: Sets the console output to the default settings. By default, the filtering condition level is critical, and sending event messages to the console port is enabled.

`host`
: Sets the syslog server output to the default settings. By default, the filtering condition level is not specified, the time is local, and sending event messages to the syslog server is disabled.

`ipv4_address`
: Specifies the IPv4 address of the syslog server.

Mode

Global Configuration mode

Description

Use this command to set the specified log to default settings.

Confirmation Command

"SHOW LOG CONFIG" on page 172

Example

This example sets the buffered log to its default settings:

```
awplus> enable
awplus# configure terminal
awplus(config)# default log buffered
```

LOG

Syntax

```
log buffered|permanent|console|host ipv4_address
```

Parameters

`buffered`
: Logs event messages in the buffered log that is stored in RAM on the switch. This is the default setting.

`permanent`
: Logs event messages in the permanent log which are stored in Flash memory on the switch. This is the default setting.

`console`
: Sends event messages to the Console port. This is the default setting.

`host`
: Sends event messages to a syslog server that you specify by its IPv4 address.

`ipv4_address`
: Specifies the IPv4 address of the syslog server.

Mode

Global Configuration mode

Description

Use this command to specify the location where log or event messages are sent.

Confirmation Command

"SHOW LOG CONFIG" on page 172

Example

This example activates the switch to send event messages to the syslog server with the IPv4 address of 192.168.10.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 192.168.10.2
```

LOG (FILTER)

Syntax

```
log buffered|permanent|monitor|console|host ipv4_address
[level level|program program_name|msgtext text_string]
```

Parameters

`buffered`
Adds filtering criteria to the buffered log.

`permanent`
Adds filtering criteria to the permanent log.

`monitor`
Adds filtering criteria to the terminal monitor log.

`console`
Adds filtering criteria to the console log.

`host`
Adds filtering criteria to the syslog server.

`ipv4_address`
Specifies the IPv4 address of the syslog server.

`level`
Specifies one of eight message levels as a filtering criterion. You can specify either a keyword or level number, where 0 is the highest level and 7 is the lowest level. The switch sends event messages with the specified level and higher levels than the specified level.

- emergency: Specifies the emergency level of event messages that the switch sends to the destination. The emergency level message is the highest level and indicates the system is not usable. Emergency is defined as level number 0.
- alert: Specifies the alert level of event messages that the switch sends to the destination. The alert level messages indicates that the system needs an immediate attention. Alert is defined as level number 1.
- critical: Specifies the critical level of event messages that the switch sends to the destination. Critical is defined as level number 2.

- error: Specifies the error level of event messages that the switch sends to the destination. Error is defined as level number 3.
- warning: Specifies the warning level of event messages that the switch sends to the destination. Warning is defined as level number 4.
- notice: Specifies the notice level of event messages that the switch sends to the destination. Notice is defined as level number 5.
- informational: Specifies the informational level of event messages that the switch sends to the destination. Informational is defined as level number 6.
- debugging: Specifies the debugging level of event messages that the switch sends to the destination. Debugging is defined as level number 7.

program_name

Specifies the name of the program that generates event messages that you want the switch to send to the destination. If you do not specify a program name, the switch sends the messages that all the programs generate to the destination. Use the SHOW LOG and SHOW LOG PERMANENT commands to list the program names that you can specify. See "SHOW LOG" on page 170 and "SHOW LOG PERMANENT" on page 175.

text_string

Specifies the text that the switch filters event message with. The textline is case-sensitive and can be up to 255 alphanumeric characters including spaces. Exclamation marks (!) and question marks (?) are not permitted.

Mode

Global Configuration mode

Description

Use this command to specify filtering criteria to the specified destination. You can filter messages based on level, program, message text, or a combination of these parameters.

To remove filtering criteria from the destination, use the NO LOG (FILTER) command.

Confirmation Command

"SHOW LOG CONFIG" on page 172

Examples

This example configures the switch to send event messages that have levels 0 to 5 and are generated by the program LACP to the syslog server with the IPv4 address of 192.168.10.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 192.168.10.2 level 5
awplus(config)# log host 192.168.10.2 program lacp
```

This example stops filtering event messages with LACP-generated messages to the destination syslog server with the IPv4 address of 192.168.10.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log host 192.168.10.2 program lacp
```

LOG HOST TIME

Syntax

```
log host ipv4_address time local|local-offset|utc-offset
plus|minus hours
```

Parameters

ipv4_address
: Specifies the IPv4 address of the syslog server.

`local`
: Specifies that the time settings of the switch and syslog server are the same. This is the default setting. When specifying the key word "local," do not specify any of the following parameters.

`local-offset`
: Specifies that the time settings of the switch and syslog server are different. Specify the time difference with the plus or minus key words followed by the number of hours.

`utc-offset`
: Specifies the time setting for the syslog server and the Coordinated Universal Time (UTC) are different. Specify the time difference with the plus or minus key words followed by the number of hours.

`plus`
: Adds the number of hours to the local-offset or utc-offset.

`minus`
: Subtracts the number of hours from the local-offset or utc-offset.

hours
: Specifies the number of hours that you want to add to or subtract from the local-offset or utc-offset. The range is 1 to 24.

Mode

Global Configuration mode

Description

Use this command to specify the time for the event messages that are sent to the syslog server. When the time settings of the switch and the syslog server are different, the switch uses the time specified by this command for event messages sent to the syslog server.

Confirmation Command

“SHOW LOG CONFIG” on page 172

Examples

This example sets the time for event messages stored in the syslog server to three hours ahead of the switch’s time. The syslog’s IPv4 address is 10.10.10.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 10.10.10.2 time local-offset plus 3
```

This example sets the time for event messages stored in the syslog to 12 hours ahead of the UTC. The syslog’s IPv4 address is 172.16.10.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 172.16.10.2 time utc-offset plus 12
```

LOG SIZE

Syntax

```
log buffered|permanent size memory_size
```

Parameters

`buffered`
: Specifies the maximum memory size of the buffered log.

`permanent`
: Specifies the maximum memory size of the permanent log.

`memory_size`
: Specifies the maximum number of memory, in Kbytes, that the switch stores event messages. The range is 50 to 250 Kbytes. By default, this value is 50 Kbytes.

Mode

Global Configuration mode

Description

Use this command to specify the maximum size of memory in Kbytes that the switch stores event messages for either the buffered or permanent logs.

Confirmation Command

"SHOW LOG CONFIG" on page 172

Example

This example specifies the maximum memory size for the permanent log is 200 Kbytes:

```
awplus> enable
awplus# configure terminal
awplus(config)# log permanent size 200
```

NO LOG

Syntax

`no log buffered|permanent|console|host` *ipv4_address*

Parameters

`buffered`
Stops logging event messages in the buffered log in RAM on the switch. By default, the switch stores event messages in the buffered log.

`permanent`
Stops logging event messages in the permanent log in Flash memory on the switch. By default, the switch stores event messages in the permanent.

`console`
Stops sending event messages defined as the console log to the Console port. By default, the switch sends these event messages to the Console port.

`host`
Stops sending event messages to a syslog server that you specify by its IPv4 address.

ipv4_address
Specifies the IPv4 address of the syslog server.

Mode

Global Configuration mode

Description

Use this command to instruct the switch to stop sending event messages to the specified destination.

Confirmation Command

“SHOW LOG CONFIG” on page 172

Examples

This example stops the switch from sending event messages defined as the console log to the Console port:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log console
```

This example stops the switch from sending event messages to the syslog server with the IPv4 address of 192.168.10.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log host 192.168.10.2
```

SHOW LOG

Syntax

```
show log [tail [value]|reverse]
```

Parameters

`tail`
: Displays the newest event messages in the buffered log in the RAM. When you do not specify the value parameter, the command displays 20 messages.

value
: Specifies the number of the newest event messages to display. The range is 10 to 250 messages. By default, this value is 20.

`reverse`
: Displays the event messages in the buffered log (that are stored in RAM) in the order of the newest to oldest message. When you do not specify this key word, the command displays the log messages from the oldest to newest message.

Mode

Privileged Exec mode

Description

Use this command to display the messages in the buffered log located in RAM on the switch. To cancel the display, type ‘q’ for quit. An example of the command output is shown in Figure 32.

```
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-------------------------------------------------------------------------
2011 Nov 15 14:39:04 user.information awplus system: Warm Boot....
2011 Nov 15 14:39:04 user.information awplus evlog: Event log initialized
2011 Nov 15 14:39:04 user.information awplus file: File System initialized
2011 Nov 15 14:39:04 user.information awplus ssh: SSH server disabled
.....
```

Figure 32. SHOW LOG Command

The fields in the log are described below:

Table 24. SHOW LOG Command

Field	Description
Date	Indicates the date the message was entered in the buffered log.
Time	Indicates the time the message was entered in the buffered log.
Facility	This field always displays "user."
Severity	Indicates 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. ❒ Warning: The issue reported by the message may require manager attention. ❒ Debug: Messages intended for technical support and software development.
Program[<pid>]	Indicates the program that generated the event message.
Message	Displays the event message.

Examples

This example displays the event messages in the buffered log from oldest to newest:

```
awplus# show log
```

This example displays 15 newest event messages in the buffered log:

```
awplus# show log tail 15
```

This example displays the event messages in the buffered log from newest to oldest:

```
awplus# show log reverse
```

SHOW LOG CONFIG

Syntax

```
show log config
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the configurations of event logs. See Figure 33 for an example of the information the command displays.

```
Buffered log:
   Status ....... enabled
   Maximum size.. 50kb (7.3kb in use)
   Filters:
*  1  Level...... informational (6)
      Program.... any
      Msg text... any
   Statistics.... 106 messages received, 82 accepted by filter
                  (2012 Aug 25 05:01:14)

Permanent log:
   Status ....... enabled
   Maximum size.. 50kb (3.2kb in use)
   Filters:
*  1  Level...... warning (4)
      Program.... any
      Msg text... any
   Statistics.... 106 messages received, 1 accepted by filter
                  (2012 Aug 25 05:01:14)

Host 172.17.28.186:
   Time offset .. +00:00
   Offset type... Local
   Filters:
*  1  Level...... any
      Program.... any
      Msg text... any
   Statistics.... 3 messages received, 3accepted by filter
                  (2012 Aug 25 05:01:14)
```

Figure 33. SHOW LOG CONFIG Command

The fields in the display are described below:

Table 25. SHOW LOG CONFIG Command

Field	Description
Log	Displays the log name or log destination. The options are: ❒ Buffered log ❒ Permanent log ❒ Host and IP address ❒ Monitor log ❒ Console log
Status	Displays whether the log output is enabled or disabled.
Maximum size	Displays the maximum size that the log can store log messages and current usage. This field is only for buffered and permanent logs.
Time offset	Displays the difference in time settings between the syslog server and the offset configured. The difference in time is indicated by the plus (+) or minus (-) number of hours. This field is only for the host (syslog server).
Offset type	Displays the setting of the standard time. The options are: ❒ Local (the switch's time zone) ❒ UTC
Filters	Displays the setting of filtering criteria. The * indicates the default setting.
Level	Displays the message level severity.
Program	Displays the name of a program that generates event messages. The keyword "any" indicates all programs.
Msg text	Displays the message text that filters event messages. The keyword "any" indicates all messages.
Statistics	Displays the number of event messages that the destination received, the number of output messages, and the time that the last message was sent.

Example

This example displays the event log settings:

```
awplus# show log config
```

SHOW LOG PERMANENT

Syntax

```
show log permanent [tail [value]]
```

Parameters

`tail`
: Displays the newest event messages in the permanent log that reside in Flash memory. When no *value* parameter is specified, the command displays 20 messages.

value
: Specifies the number of the newest event messages to display. The range is 10 to 250 messages. By default, this value is 20.

Mode

Privileged Exec mode

Description

Use this command to display the messages in the permanent log stored in the Flash memory of the switch. To cancel the display, type 'q' for quit. See Figure 34 for an example of the command output.

```
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-------------------------------------------------------------------------
2011 Oct 22 14:39:04 user.error awplus system: Fan3 Status fault
2011 Oct 26 11:15:02 user.error awplus enco: key file a.cfg to node failed[565]
2011 Nov 15 13:40:11 user.warning awplus rmon: RMON falling threshold reached
2011 Nov 15 14:55:04 user.error awplus vlan: VLAN Creation failed[236]
2011 Nov 15 14:55:45 user.error awplus vlan: VLAN Creation failed[236]
```

Figure 34. SHOW LOG Permanent Command

The fields in the log are described below:

Table 26. SHOW LOG Permanent Command

Field	Description
Date	Indicates the date the message was entered in the permanent log.
Time	Indicates the time the message was entered in the permanent log.

Table 26. SHOW LOG Permanent Command (Continued)

Field	Description
Facility	This field always displays “user.”
Severity	Indicates 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. ❒ Warning: The issue reported by the message may require manager attention. ❒ Debug: Messages intended for technical support and software development.
Program[<pid>]	Indicates the program that generated the event message.
Message	Displays the event message.

Examples

This example displays the event messages in the permanent log from oldest to newest:

```
awplus# show log permanent
```

This example displays 15 newest event messages in the permanent log:

```
awplus# show log permanent tail 15
```

TERMINAL MONITOR

Syntax

```
terminal monitor
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to output event messages defined as the monitor log on the Console monitor. By default, the switch outputs event messages with all levels. You can change the event message filtering criteria using the LOG (FILTER) command. See "LOG (FILTER)" on page 162.

To stop displaying event messages on the Console monitor, use the TERMINAL NO MONITOR command.

Note
You can execute the TERMINAL MONITOR and TERMINAL NO MONITOR commands from remote management sessions; however, the switch displays event messages defined as the monitor log only on the console monitor.

Examples

This example outputs event messages on the console terminal.

```
awplus# terminal monitor
```

This example stops displaying event messages on the console terminal.

```
awplus# terminal no monitor
```

Chapter 8
SNMP Commands

The SNMPv1, SNMPv2c, and SNMPv3 commands are summarized in Table 27.

Table 27. SNMPv1, SNMPv2c, SNMPv3 Commands

Command	Mode	Description
“NO SNMP-SERVER” on page 181	Global Configuration	Disables SNMPv1 and SNMPv2c on the switch.
“NO SNMP-SERVER COMMUNITY” on page 182	Global Configuration	Deletes SNMPv1 and SNMPv2c community strings.
“NO SNMP-SERVER CONTACT” on page 183	Global Configuration	Deletes the value of the MIB object sysContact.
“NO SNMP-SERVER ENABLE TRAP” on page 184	Global Configuration	Disables the transmission of authentication traps, RMON traps, or both.
“NO SNMP-SERVER ENGINEID LOCAL” on page 185	Global Configuration	Removes the user-defined SNMPv3 engine ID.
“NO SNMP-SERVER GROUP” on page 186	Global Configuration	Deletes an SNMPv3 group.
“NO SNMP-SERVER HOST” on page 187	Global Configuration	Removes a trap or inform recipient.
“NO SNMP-SERVER LOCATION” on page 189	Global Configuration	Removes the value of the MIB object sysLocation.
“NO SNMP-SERVER USER” on page 190	Global Configuration	Deletes an SNMPv3 user.
“NO SNMP-SERVER VIEW” on page 191	Global Configuration	Deletes an SNMP view.
“NO SNMP TRAP LINK-STATUS” on page 192	Port Interface	Disables the transmission of SNMP link status traps when ports establish links or lose links to network devices.
“SHOW SNMP-SERVER” on page 193	Privileged Exec	Displays the current status of the SNMP agent on the switch.

Table 27. SNMPv1, SNMPv2c, SNMPv3 Commands (Continued)

Command	Mode	Description
“SHOW SNMP-SERVER COMMUNITY” on page 195	Privileged Exec	Displays the SNMPv1 and SNMPv2c community strings and their settings.
“SHOW SNMP-SERVER GROUP” on page 196	Privileged Exec	Displays the SNMPv3 groups and their settings.
“SHOW SNMP-SERVER USER” on page 198	Privileged Exec	Displays the SNMPv3 users and their settings.
“SHOW SNMP-SERVER VIEW” on page 199	Privileged Exec	Displays the SNMPv3 views and their settings.
“SNMP-SERVER” on page 200	Global Configuration	Enables the SNMPv1, SNMPv2c, and SNMPv3 agent on the switch.
“SNMP-SERVER COMMUNITY” on page 201	Global Configuration	Creates new SNMPv1 and SNMPv2c community strings.
“SNMP-SERVER CONTACT” on page 202	Global Configuration	Sets the value of the MIB object sysContact.
“SNMP-SERVER ENABLE TRAP” on page 203	Global Configuration	Activates the transmission of authentication traps, RMON traps, or both.
“SNMP-SERVER ENGINEID LOCAL” on page 205	Global Configuration	Sets or modifies the user-defined SNMPv3 engine ID.
“SNMP-SERVER GROUP” on page 206	Global Configuration	Creates SNMPv3 groups.
“SNMP-SERVER HOST” on page 208	Global Configuration	Adds a trap or inform recipient.
“SNMP-SERVER LOCATION” on page 210	Global Configuration	Sets or modifies the value of the MIB object sysLocation.
“SNMP-SERVER USER” on page 211	Global Configuration	Creates a new SNMPv3 user.
“SNMP-SERVER VIEW” on page 213	Global Configuration	Creates an SNMP view.
“SNMP TRAP LINK-STATUS” on page 214	Port Interface	Configures SNMP to transmit link status traps 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 the SNMPv1, SNMPv2c, and SNMPv3 agent on the switch. The switch does not permit remote management from SNMP applications when SNMP is disabled.

Confirmation Command

"SHOW SNMP-SERVER" on page 193.

Example

This example disables the SNMPv1, SNMPv2c, and SNMPv3 agent 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 SNMPv1 or SNMPv2c community string. This parameter is case-sensitive.

Mode

Global Configuration mode

Description

Use this command to delete an SNMPv1 or SNMPv2c community string from the switch.

Confirmation Command

“SHOW SNMP-SERVER COMMUNITY” on page 195

Example

This example deletes the “browsers” community string from the switch:

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

NO SNMP-SERVER CONTACT

Syntax

```
no snmp-server contact
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to delete the value of the MIB object sysContact.

Confirmation Command

"SHOW SYSTEM" on page 119

Example

This example deletes the value of the MIB object sysContact:

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

NO SNMP-SERVER ENABLE TRAP

Syntax

```
no snmp-server enable trap [auth|rmon]
```

Parameters

`auth`
: Specifies SNMP authentication traps.

`rmon`
: Specifies Remote Monitoring (RMON) SNMP traps.

Mode

Global Configuration mode

Description

Use this command to disable the transmission of authentication traps, RMON traps, or both. If you do not specify a keyword, the command disables *both* authentication traps and RMON traps.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example disables the transmission of SNMP authentication traps:

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

This example disables the transmission of both SNMP authentication traps and RMON traps:

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

NO SNMP-SERVER ENGINEID LOCAL

Syntax

```
no snmp-server engineid local
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to remove the user-defined SNMPv3 engine ID. By default, the engine ID is set a random number.

Confirmation Command

"SHOW SNMP-SERVER" on page 193

Example

This example removes the user-defined SNMPv3 engine ID:

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

NO SNMP-SERVER GROUP

Syntax

```
no snmp-server group name auth|priv|noauth
```

Parameters

name
: Specifies the name of the group. The name is case-sensitive.

`auth`
: Specifies the group's minimum security level as authentication without encryption.

`priv`
: Specifies the group's minimum security level as privacy. Privacy means that the members of this group are required for authentication with encryption.

`noauth`
: Specifies the group's minimum security level as no authentication.

Mode

Global Configuration Mode

Description

Use this command to delete an SNMPv3 group.

Examples

This example deletes the group called "admins" which has the minimum security level of authentication with encryption:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server group admins priv
```

This example deletes the group called "operators" which has the minimum security level of authentication without encryption:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server group operators auth
```

NO SNMP-SERVER HOST

Syntaxes

`no snmp-server host` *`ipaddress`* `traps version 1` *`community`*

`no snmp-server host` *`ipaddress`* `traps|informs version 2c` *`community`*

`no snmp-server host` *`ipaddress`* `traps|informs version 3 auth|priv|noauth` *`user`*

Parameters

`ipaddress`
: Specifies the IPv4 address of a recipient of SNMP trap or inform notifications that the switch sends.

`traps`
: Specifies traps as the message type. With SNMP version 1, the message type can only be traps.

`informs`
: Specifies informs as the message type.

community
: Specifies an SNMPv1 and SNMPv2c community string. A community string is case-sensitive. When version 1 or 2c is specified, you must specify a community string.

`auth`
: Specifies authentication as the minimum security level. When version 3 is specified, you must specify authentication, privacy, or no authentication.

`priv`
: Specifies privacy as the minimum security level. When version 3 is specified, you must specify authentication, privacy, or no authentication.

`noauth`
: Specifies no authentication as the minimum security level. When version 3 is specified, you must specify authentication, privacy, or no authentication.

user
: Specifies the name of an SNMPv3 user. The name is case-sensitive.

Mode

Global Configuration mode

Description

Use this command to remove a trap or inform receiver from the switch.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Examples

This example deletes a trap recipient with the IPv4 address 192.168.10.102, the SNMPv1 format, and the community string “private”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 192.168.10.102 traps
version 1 private
```

This example deletes an inform recipient with the IPv4 address 10.10.10.224, the SNMPv2c format, and the community string “viewers”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 10.10.10.224 informs
version 2c viewers
```

This example deletes a trap recipient with the IPv4 address 172.16.10.12, the security level “authentication, and the user name “jsmith”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 172.16.100.12 traps
version 3 auth jsmith
```

NO SNMP-SERVER LOCATION

Syntax

```
no snmp-server location
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to remove the value of the MIB object sysLocation.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example removes the value of the MIB object sysLocation:

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

NO SNMP-SERVER USER

Syntax

```
no snmp-server user
```

Parameter

user
: Specifies the name for an SNMPv3 user to delete. A name is case-sensitive.

Mode

Global Configuration mode

Description

Use this command to delete an SNMP user. You can delete one user at a time with this command.

Confirmation Command

“SHOW SNMP-SERVER USER” on page 198

Example

This example deletes the user “jsmith”:

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

NO SNMP-SERVER VIEW

Syntax

```
no snmp-server view viewname oid
```

Parameters

viewname
Specifies the name of the view. The name is case-sensitive.

oid
Specifies the OID of the view.

Mode

Global Configuration mode

Description

Use this command to delete an SNMP view. You can delete only one view at a time with this command.

Confirmation Command

"SHOW SNMP-SERVER VIEW" on page 199

Example

This example deletes the view called "standard" with an OID of 1.3.6.1:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server view standard 1.3.6.1
```

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 traps “linkUp” and “linkDown” when ports establish links or lose links to network devices.

Confirmation Command

“SHOW INTERFACE” on page 260

Example

This example disables the transmission of link status traps on ports 1.0.17 and 1.0.21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17,port1.0.21
awplus(config-if)# no snmp trap link-status
```

SHOW SNMP-SERVER

Syntax

```
show snmp-server
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the current status of the SNMP agent on the switch. See Figure 35 for an example.

```
SNMP Server ....... Enabled
IP Protocol ....... IPv4
SNMPv3 Engine ID (Configured) ........ Not set
SNMPv3 Engine ID (actual) ............ 0x80001f8880793499cd7bdba40e
```

Figure 35. SHOW SNMP-SERVER Command

The fields are described in Table 28.

Table 28. SHOW SNMP-SERVER Command

Field	Description
SNMP Server	Indicates whether the SNMP agent on the switch is enabled or disabled.
IP Protocol	Displays the IP protocol that the switch supports. The switch currently supports only IPv4.
SNMPv3 Engine ID <Configured>	Displays the SNMPv3 engine ID that you set with the SNMP-SERVER ENGINEID LOCAL command.
SNMPv3 Engine ID <Actual>	Displays the SNMPv3 engine ID that the switch is currently using.

Example

This example displays the current status of the SNMP agent:

```
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 and their settings 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 36. SHOW SNMP-SERVER COMMUNITY Command

The fields in the entries are described in Table 29.

Table 29. SHOW SNMP-SERVER COMMUNITY Command

Parameter	Description
Community Name	Displays the community string.
Access	Displays the access level of the community string. The options are: ❒ Read-Write ❒ Read-Only.
View	Not supported. Always displays none.

Example

This example displays the SNMPv1 and SNMPv2c community strings and their settings:

```
awplus# show snmp-server community
```

SHOW SNMP-SERVER GROUP

Syntax

```
show snmp-server group
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display SNMPv3 groups and their settings on the switch. Figure 37 shows an example.

```
SNMP group information:
   Group Name .............admins
      Security Level ......priv
      Read View ...........most
      Write View ..........most
      Notify View .........most

   Group Name .............operators
      Security Level ......auth
      Read View ...........standard
      Write View ..........none
      Notify View .........none
```

Figure 37. SHOW SNMP-SERVER GROUP Command

The fields in the entries are described in Table 30.

Table 30. SHOW SNMP-SERVER GROUP Command

Parameter	Description
Group Name	Displays the group name.
Security Level	Displays the security level of the group. The options are: ❒ auth: authentication ❒ priv: authentication and encryption ❒ noauth: no authentication

Table 30. SHOW SNMP-SERVER GROUP Command (Continued)

Parameter	Description
Read View	Displays the name of the view that defines the MIB objects the group members can read.
Write View	Displays the name of the view that defines the MIB objects the group members can write.
Notify View	Displays the name of the view that defines the MIB objects the group members receive by notifications.

Example

This example displays SNMPv3 groups and their settings on the switch:

```
awplus# show snmp-server group
```

SHOW SNMP-SERVER USER

Syntax

```
show snmp-server user
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv3 users and their settings on the switch. See Figure 38 for an example.

```
Name                                Auth        Privacy
-------                             -------     ----------
supervisor                          SHA         DES
administrator                       MD5         DES
zein                                MD5         none
```

Figure 38. SHOW SNMP-SERVER USER Command

The fields in the entries are described in Table 31.

Table 31. SHOW SNMP-SERVER USER Command

Field	Description
Name	Displays the user name.
Auth	Displays the authentication algorithm.
Privacy	Displays the encryption algorithm.

Example

The following example displays the SNMPv3 users and their settings:

```
awplus# show snmp-server user
```

SHOW SNMP-SERVER VIEW

Syntax

```
show snmp-server view
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the SNMPv3 views on the switch. See Figure 39 for an example.

```
SNMP V3 View information:
   View Name ............. most
      OID ................ 1.3.6.1
      Type ............... included

   View Name ............. standard
      OID ................ 1.3.6.1.2.1
      Type ............... included
```

Figure 39. SHOW SNMP-SERVER VIEW Command

The fields are described in Table 32.

Table 32. SHOW SNMP-SERVER VIEW Command

Field	Description
View Name	Displays the view name.
OID	Displays the OID to a section of the MIB tree.
Type	Displays the view type, which is included.

Example

The following 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 enable the SNMP agent on the switch. The switch permits remote management from SNMP applications when SNMP is enabled. By default, the SNMP agent is disabled.

Confirmation Command

“SHOW SNMP-SERVER” on page 193

Example

This example enables the SNMPv1, SNMPv2c, and SNMPv3 agent 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 community string is case-sensitive and can be up to 20 alphanumeric characters. Spaces, exclamation marks (!), and question marks (?) are *not* permitted.

rw
: Specifies the access level of read-write (rw) to a community string.

ro
: Specifies the access level of read-only (ro) to a community string.

Mode

Global Configuration mode

Description

Use this command to create a SNMPv1 and SNMPv2c community string on the switch. The community string is as a password for SNMP network management systems to communicate with the switch. If you do not specify the access level, a new community string is created with the "ro" access level.

Confirmation Command

"SHOW SNMP-SERVER COMMUNITY" on page 195

Example

This example creates the new community string, "browsers," with an access level of read-only:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server community browsers ro
```

SNMP-SERVER CONTACT

Syntax

```
snmp-server contact contact
```

Parameter

contact
: Specifies a system administrator's contact information. The maximum length is 255 alphanumeric characters. This parameter is case-sensitive. Special characters are permitted with the exception of exclamation marks (!) and question marks (?).

Mode

Global Configuration mode

Description

Use this command to set the value of the MIB object sysContact.

Confirmation Command

"SHOW SYSTEM" on page 119

Example

This example sets the value of the MIB object sysContact to "admin@alliedtelesis.com":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server contact admin@alliedtelesis.com
```

SNMP-SERVER ENABLE TRAP

Syntax

```
snmp-server enable trap [auth|rmon]
```

Parameters

`auth`
: Specifies SNMP authentication traps.

`rmon`
: Specifies RMON SNMP traps for remote monitoring.

Mode

Global Configuration mode

Description

Use this command to enable the transmission of SNMP notifications of authentication traps, remote monitoring (RMON) traps, or both. If you do not specify a parameter when you enter this command, the software enables *both* authenticator traps and RMON traps. By default, the transmission of both authentication traps and RMON traps is disabled.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example enables the transmission of both authentication traps and RMON traps:

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

This example enables the transmission of only authentication traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server enable trap auth
```

This example activates the transmission of both authentication traps and RMON traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server enable trap auth rmon
```

SNMP-SERVER ENGINEID LOCAL

Syntax

```
snmp-server engineid local engine-id|default
```

Parameters

engine-id
: Specifies the user-defined SNMPv3 engine ID (MIB object snmpEngineID). The value can be up to 32 alphanumeric characters. By default, the engine ID is set a random number.

`default`
: Returns the default value. The engine ID is removed if a value was set. This command with the default keyword is equivalent to the "NO SNMP-SERVER ENGINEID LOCAL" on page 185.

Mode

Global Configuration mode

Description

Use this command to set or modify the user-defined SNMPv3 engine ID. The SNMP engine ID is used to identify the device for administrative purposes only.

Confirmation Command

"SHOW SNMP-SERVER" on page 193

Examples

This example sets the user-defined SNMPv3 engine ID to 89ab532d782:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server engineid local 89ab532d782
```

This example removes the user-defined SNMPv3 engine ID:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server engineid local default
```

SNMP-SERVER GROUP

Syntax

```
snmp-server group groupname auth|priv|noauth read readview|
write writeview|notify notifyview
```

Parameters

groupname
: Specifies a name of an SNMPv3 group. The name is case-sensitive and can consist of up to 20 alphanumeric characters. Spaces, exclamation marks (!), and question marks (?) are *not* permitted.

`auth`
: Specifies the minimum group security level as authentication without encryption. You must assign users who belong to this group at least this level of security with the SNMP-SERVER USER command.

`priv`
: Specifies the minimum group security level as privacy which means authentication with encryption. You must assign users who belong to this group at least this level of security with the SNMP-SERVER USER command.

`noauth`
: Specifies the minimum group security level as no authentication. The users who belong to this group are not required to have any specified security level. You define users with the SNMP-SERVER USER command.

readview
: Specifies the name of an existing SNMPv3 view that defines the MIB objects the group members can view. If you omit this parameter, the members cannot view any MIB objects using the group. The name is case-sensitive. You define SNMPv3 views with the SNMP-SERVER VIEW command.

writeview
: Specifies the name of an existing SNMPv3 view that defines the MIB objects the group members can change. If you omit this parameter, the members cannot change any MIB objects using the group. The name is case-sensitive. You define SNMPv3 views with the SNMP-SERVER VIEW command.

notifyview

Specifies the name of an existing SNMPv3 view that defines the MIB objects the group members receive as notifications. If you omit this parameter, the members cannot receive notification of any MIB objects. The name is case-sensitive. You define SNMPv3 views with the SNMP-SERVER VIEW command.

Mode

Global Configuration Mode

Description

Use this command to create an SNMPv3 group. Before you create a group, you must define the group members, who are also known as users, as well as the permitted views of MIB objects for this group.

You define users, including their security levels, with the SNMP-SERVER USER command. See "SNMP-SERVER USER" on page 211. To define whether or not a user can view, change, or receive notification of MIB objects, use the SNMP-SERVER VIEW command. See "SNMP-SERVER VIEW" on page 213.

Examples

This example creates a group called "admins." The members of this group must have a security level of authentication with encryption and can read and change MIB objects named "most":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server group admins priv read most
write most
```

This example creates a group called "operators." The members of this group must have a security level of authentication without encryption and can read MIB objects named "standard":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server group operators auth read
standard
```

SNMP-SERVER HOST

Syntaxes

`snmp-server host` *ipaddress* `traps version 1` *community*

`snmp-server host` *ipaddress* `traps|informs version 2c` *community*

`snmp-server host` *ipaddress* `traps|informs version 3 auth|priv|noauth` *user*

Parameters

ipaddress
: Specifies the IPv4 address of a recipient of an SNMP trap or inform notification sent by the switch.

`traps`
: Specifies the message type as traps. You can specify traps only for SNMPv1.

`informs`
: Specifies the message type as informs.

community
: Specifies a SNMPv1 and SNMPv2c community string. The community string must exist on the switch. This parameter is case-sensitive. Specify this parameter *only* for SNMPv1 and SNMPv2c.

`auth`
: Specifies the minimum security level for the host as authentication.

`priv`
: Specifies the minimum security level for the host as privacy. Privacy means authentication with encryption.

`noauth`
: Specifies the minimum security level for the host as no authentication.

user
: Specifies the name of an SNMPv3 user. The name is case-sensitive.

Mode

Global Configuration mode

Description

Use this command to add a trap or inform recipient by specifying the IPv4 address of a network device. The command syntax depends upon the SNMP version:

- SNMPv1: Specify the IP address of a recipient of SNMP trap, the message version, and a community string that is used for authentication.
- SNMPv2c: Specify the IP address of a recipient of SNMP trap or inform notifications, traps or informs as the message type, the message version, and a community string that is used for authentication.
- SNMPv3: Specify the IP address of a recipient of SNMP trap or inform notifications, the message type, the message version, the security level, and a user.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example assigns the IPv4 address 192.168.10.102 of a trap receiver to the community string "private." The traps are sent in the SNMPv1 format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 192.168.10.102 traps
version 1 private
```

This example assigns the IPv4 address 10.10.10.224 as an inform receiver to the community string "viewers." The traps are sent in the SNMPv2c format:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 10.10.10.224 informs
version 2c viewers
```

This example configures SNMPv3 to send trap messages to an end node with the IPv4 address 172.16.10.12. The security level is specified as authentication and the user name associated with this entry is "jsmith":

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 172.16.100.12 traps version
3 auth jsmith
```

SNMP-SERVER LOCATION

Syntax

```
snmp-server location text
```

Parameter

text

Specifies the value of the MIB object sysLocation. The maximum length is 255 alphanumeric characters. Special characters are permitted with the exception of exclamation marks (!) and question marks (?).

Mode

Global Configuration mode

Description

Use this command to set the value of the MIB object sysLocation. This value indicates the physical location of the system.

Confirmation Command

“SHOW SYSTEM” on page 119

Example

This example sets the value of the MIB object sysLocation to “San Jose 2F”:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server location San Jose 2F
```

SNMP-SERVER USER

Syntax

`snmp-server user` *`username groupname`* `[auth md5|sha` *`auth_password`*`] [priv des` *`priv_passphase`*`]`

Parameters

`username`

Specifies the name of an SNMPv3 user. The name is case-sensitive and can contain up to 20 alphanumeric characters. Spaces, exclamation marks (!), and question marks (?) are *not* permitted.

`groupname`

Specifies the name of a group for the user. Groups are defined by the "SNMP-SERVER GROUP" on page 206. A group name is case-sensitive.

`md5`

Specifies the authentication algorithm as MD5 Message-Digest Algorithm.

`sha`

Specifies the authentication algorithm as SHA (Secure Hash Algorithm).

auth_password

Specifies a password for authentication. The password is case-sensitive and can contain from 8 to 20 alphanumeric characters. Spaces, exclamation marks (!), question marks (?) are *not* permitted.

`priv`

Specifies an encryption algorithm and an encryption pass phrase. If you do not specify an authentication algorithm and password using the "auth" keyword, you are not permitted to specify an encrypted algorithm and password using the "priv" keyword.

`des`

Specifies Data Encryption Standard (DES) as the encryption algorithm. This is only algorithm option.

`priv_passphase`

Specifies a pass phrase for DES. A pass phrase is case-sensitive and can be 8 to 20 alphanumeric characters. Spaces, exclamation marks (!), question marks (?) are *not* permitted.

Mode

Global Configuration mode

Description

Use this command to create an SNMPv3 user. You can assign a user with a security level of no security, authentication only, or authentication and privacy (encryption). 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.
- 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.

Confirmation Command

“SHOW SNMP-SERVER USER” on page 198

Examples

This example creates the user “jsmith” to belong to the group “admins.” Since the minimum security level of the group “admns” is privacy, both an authentication password (ssujasha8*8*) and an encrypted password (ati345#$) are specified:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server user jsmith admins auth sha
ssujasha8*8* priv des ati345#$
```

This example creates the user “bjones” to belong to the group “operators.” Since the minimum security level of the group “operators” is authentication without encryption, an authentication password (as11fir&) is specified:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server user bjones operators auth md5
as11fir&
```

SNMP-SERVER VIEW

Syntax

```
snmp-server view viewname oid included
```

Parameters

viewname	Specifies the name of a view. A view name is case-sensitive and can be up to 20 alphanumeric characters. Spaces, exclamation marks (!), and question marks (?) are *not* permitted.
oid	Specifies the OID (object identifier) of the view. The OID must be in decimal format.

Mode

Global Configuration mode

Description

Use this command to create an SNMPv3 view or add a view entry to an existing SNMPv3 view on the switch. Views are used to restrict the MIB objects that a group of SNMP users can access. The views defined using this command are added to a definition of a group with the SNMP-SERVER GROUP command. See "SNMP-SERVER GROUP" on page 206. A view can have more than one OID, but you must enter each OID in a separate command.

Confirmation Command

"SHOW SNMP-SERVER VIEW" on page 199

Examples

This example creates a view named "standard," with includes all MIB objects under the internet node (1.3.6.1):

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view standard 1.3.6.1 included
```

This example creates a view named "admins," which includes all MIB objects under the MIB-2 node (1.3.6.1.2.1):

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view admins 1.3.6.1.2.1 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 traps “linkUp” and “linkDown” when ports establish links or lose links to network devices. By default, the transmission of link status traps is disabled.

Confirmation Command

“SHOW INTERFACE” on page 260

Example

This example configures the switch to transmit link status traps whenever links are established or lost on ports 1.0.1 through 1.0.4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# snmp trap link-status
```

Chapter 9

RMON Commands

The Remote Network MONitoring (RMON) commands are summarized in Table 33.

Table 33. RMON Commands

Command	Mode	Description
“NO RMON ALARM” on page 216	Global Configuration	Deletes RMON alarms from the switch.
“NO RMON COLLECTION STATS” on page 217	Port Interface	Deletes an RMON statistic entry on the port.
“NO RMON EVENT” on page 218	Global Configuration	Deletes RMON events from the switch.
“RMON ALARM” on page 219	Global Configuration	Creates alarms to monitor RMON statistics on the ports.
“RMON COLLECTION STATS” on page 222	Port Interface	Creates an RMON statistic entry on the specified port and enables collecting statistics.
“RMON EVENT” on page 223	Global Configuration	Defines RMON events for RMON alarms
“SHOW RMON EVENT” on page 225	Privileged Exec	Displays the settings of RMON events on the switch.
“SHOW RMON STATISTICS” on page 227	Privileged Exec	Displays the statistics groups that are assigned to the ports.

NO RMON ALARM

Syntax

```
no rmon alarm alarm_id
```

Parameter

alarm_id
: Specifies the ID number of an alarm to delete. The range is 1 to 65,535.

Mode

Global Configuration mode

Description

Use this command to delete an alarm from the switch.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example deletes the alarm with an ID of 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no rmon event 2
```

NO RMON COLLECTION STATS

Syntax

```
rmon collection stats stats_index
```

Parameter

stats_index
: Specifies the index number of a new statistic entry to delete. The range is 1 to 65,535.

Mode

Port Interface mode

Description

Use this command to delete an RMON statistic entry.

Confirmation Command

"SHOW RMON STATISTICS" on page 227

Example

This example deletes an RMON statistic entry, with an index of 2, from port 1.0.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection stats 2
```

NO RMON EVENT

Syntax

```
no rmon event event_index
```

Parameter

event_index
: Specifies the index number of the event to delete. The range is 1 to 65,535.

Mode

Global Configuration mode

Description

Use this command to delete events from the switch.

Confirmation Command

“SHOW RMON EVENT” on page 225

Example

This example deletes an RMON event of 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no rmon event 2
```

RMON ALARM

Syntax

```
rmon alarm alarm_id oid 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 65,535.

oid

Specifies an object ID number to an SNMP MIB object (alarmVariable). The object ID number is entered in the following format:

1.3.6.1.2.1.16.1.1.1.*field*.*index*

- 1.3.6.1.2.1.16.1.1.1: Specifies the ID of the MIB object "etherStatsEntry." It is always this number.
- *field*: Specifies the filed number in the MIB object "etherStatsEntry" table.
- *index*: Specifies the index number of the statistic entry (etherStatsIndex) specified by the RMON COLLECTION STATS command.

interval

Specifies the polling interval in seconds to the MIB object "alarmInterval." The range is 1 to 65,535 seconds.

`delta`

Specifies the delta type to the MIB object "alarmSampleType." The delta type compares the threshold with the difference between the current sampling value and the previous sampling value.

`absolute`

Specifies the absolute type of the MIB object "alarmSampleType." The absolute type compares the threshold with the sampling value.

`rising-threshold`

Specifies the rising threshold. The range is 1 to 65,535.

rising_event_id
: Specifies the ID number of the event that is triggered when the rising threshold is crossed. The event must be defined by the RMON EVENT command.

falling-threshold
: Specifies the falling threshold. The range is 1 to 65,535.

falling_event_id
: Specifies the ID number of the event that is triggered when the falling threshold is crossed. The event must be defined by the RMON EVENT command.

owner
: Specifies the owner of the alarm (alarmOwner). The owner can be up to 20 alphanumeric characters.

Mode

Global Configuration mode

Description

Use this command to set RMON alarms by creating an entry in the SNMP MIB alarm table. RMON is a standard monitoring specification, which is an extension of the SNMP MIB. RMON alarms monitor the values of SNMP objects and trigger events when the values of the monitored objects cross specified thresholds.

Before setting an RMOM alarm, you must specify statistic entries and RMON events. See “RMON COLLECTION STATS” on page 222 and “RMON EVENT” on page 223.

Configuring RMON is more common and easier using an SNMP manager than using the CLI commands on the switch.

Confirmation Command

“SHOW RMON EVENT” on page 225

Example

This example defines RMON events that send SNMP traps, creates an statistic entry, and sets an RMON alarm that monitors the ingress packets on port 1.0.2. The alarm sends SNMP traps if the number of packets exceeds 3,000 packets per minute or falls below 2,000 packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# rmon event 21 log trap managers description
rxmin_rise_3000
```

```
awplus(config)# rmon event 22 log trap managers description
rxmin_fall_2000
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection stats 2
awplus(config-if)# exit
awplus(config)# rmon alarm 2 1.3.6.1.2.1.16.1.1.1.5.2
interval 60 delta rising-threshold 3000 event 21 falling-
threshold 2000 event 22
```

RMON COLLECTION STATS

Syntax

```
rmon collection stats stats_index [owner owner]
```

Parameters

stats_index
: Specifies the index number of a new statistic entry (etherStatsIndex). The range is 1 to 65,535.

owner
: Specifies the owner of the statistic entry (etherStatsOwner). The owner can be up to 20 alphanumeric characters.

Mode

Port Interface mode

Description

Use this command to create an RMON statistic entry to enable collecting statistics on the specified port for RMON alarms. RMON is a standard monitoring specification, which is an extension of the SNMP MIB. You must create an RMON statistic entry before creating RMON alarms. See “RMON ALARM” on page 219.

Configuring RMON is more common and easier using an SNMP manager than using the CLI commands on the switch.

Confirmation Command

“SHOW RMON STATISTICS” on page 227

Example

This example creates an RMON statistic entry, with an index of 2, to enable collecting statistics on port 1.0.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection stats 2
```

RMON EVENT

Syntax

```
rmon event event_index type [description description]
[owner owner]
```

Parameters

event_index
Specifies the index number of the event. The range is 1 to 65,535.

type
Specifies the event type (eventType). The options are:

- log:
- trap *community*.
- log trap *community*.

description
Specifies the description of the event (eventDescription). The description can be up to 120 alphanumeric characters.

owner
Specifies the owner of the event (eventOwner). The description can be up to 120 alphanumeric characters.

Mode

Port Interface mode

Description

Use this command to defines RMON events for RMON alarms. RMON is a standard monitoring specification, which is an extension of the SNMP MIB. You must create RMON events before creating RMON alarms. See "RMON ALARM" on page 219.

Configuring RMON is more common and easier using an SNMP manager than using the CLI commands on the switch.

Confirmation Command

"SHOW RMON EVENT" on page 225

Example

This example defines the RMON event 21 that logs the event sends traps to the community “managers” when an alarm goes off:

```
awplus> enable
awplus# configure terminal
awplus(config)# rmon event log trap managers description
sample_event_entry
```

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. See Figure 40 for an example of the information.

```
Event index = 21
   Description rxmin_rise_3000
   Event type log & trap
   Event community name managers
   Last Time Sent = 0
   Owner Agent
Event index = 22
   Description rxmin_fall_2000
   Event type log & trap
   Event community name managers
   Last Time Sent = 0
   Owner Agent
```

Figure 40. SHOW RMON EVENT Command

The fields are described in Table 34.

Table 34. SHOW RMON EVENT Command

Field	Description
Event index	Displays the index number of the event.
Description	Displays the description of the event.

Table 34. SHOW RMON EVENT Command (Continued)

Field	Description
Event type	Displays the event type. The types are: ❒ log - The event enters in the event log. ❒ trap - The event sends an SNMP trap. ❒ log & trap - The event enters in the event log and sends an SNMP trap. ❒ Log & Trap - The event enters a message in the event log and sends an SNMP trap.
Event community name	Displays the community string for sending SNMP traps.
Last Time Sent	Not supported.
Owner	Displays the owner of the event. The owner is Agent if no owner was specified when the event was created.

Example

This example displays the RMON events on the switch:

```
awplus# show rmon event
```

SHOW RMON STATISTICS

Syntax

```
show rmon statistics
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the RMON statistics on the switch. See Figure 41 for an example of the command.

```
Stats Index = 2
   Data source ifindex = 2
   Owner Agent
```

Figure 41. SHOW RMON STATISTICS Command

The fields are described in Table 35.

Table 35. SHOW RMON STATISTICS Command

Field	Description
Stats Index	Displays the index number of the statistic entry.
Data source ifindex	Displays the index number of port interfaces that the statistics are collected on.
Owner	Displays the owner of the statistic entry. The owner is Agent if no owner was specified when the statistics entry was created.

Example

This example displays the RMON statistics on the switch:

```
awplus# show rmon statistics
```

Chapter 10
NTP Client Commands

The NTP commands are summarized in Table 36.

Table 36. Simple Network Time Protocol Commands

Command	Mode	Description
“CLOCK TIMEZONE” on page 230	Global Configuration	Sets the UTC offset value, the time difference in hours and minutes between local time and Coordinated Universal Time (UTC).
“NO NTP PEER” on page 231	Global Configuration	Disables the NTP client.
“NTP PEER” on page 232	Global Configuration	Specifies the IP address of the NTP server where the switch obtains the date and time.
“PURGE NTP” on page 233	Global Configuration	Restores the default settings to the NTP client.
“SHOW NTP ASSOCIATIONS” on page 234	Privilege Exec	Displays the settings of the NTP client on the switch.
“SHOW NTP STATUS” on page 236	Privilege Exec	Displays whether the switch has synchronized its time with the specified NTP server.

CLOCK TIMEZONE

Syntax

```
clock timezone +hh:mm|-hh:mm
```

Parameter

hh:mm

Specifies the number of hours and minutes 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 00 to 60. 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 NTP server into local time. You must configure the NTP client with “NTP PEER” on page 232 before setting the UTC offset.

To remove the UTC offset and set the time zone to UTC, use the NO CLOCK TIMEZONE command.

Confirmation Commands

“SHOW NTP ASSOCIATIONS” on page 234 and “SHOW NTP STATUS” on page 236

Examples

This example specifies a time difference of -7 hours between UTC and local time:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock timezone -07:00
```

This example sets the time zone to the default UTC:

```
awplus> enable
awplus# configure terminal
awplus(config)# no clock timezone
```

NO NTP PEER

Syntax

```
no ntp peer
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the NTP client on the switch.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 234

Example

This example deactivates the NTP 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 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 NTP server. The switch obtains its date and time from the NTP server. You can specify only one 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 234

Example

This example activates the NTP client on the switch and defines the IP address of the NTP server as 172.17.28.251:

```
awplus> enable
awplus# configure terminal
awplus(config)# ntp peer 172.17.28.251
```

PURGE NTP

Syntax

```
purge ntp
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the NTP client, delete the IP address of the NTP server, and restore the client settings to the default values.

Confirmation Command

"SHOW NTP ASSOCIATIONS" on page 234

Example

This example disables the NTP client, deletes the IP address of the NTP server, and restores the client settings to the default values:

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

SHOW NTP ASSOCIATIONS

Syntax

```
show ntp associations
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display the settings of the NTP client. See Figure 42 for information the command displays.

```
NTP Configuration:
   Status ..................... Enabled
   Server ..................... 172.17.118.15
   UTC Offset ................. -07:00
   Daylight Savings Time (DST) ... Disabled
```

Figure 42. SHOW NTP ASSOCIATIONS Command

The information is described here:

Table 37. SHOW NTP ASSOCIATIONS Command

Field	Description
Status	Displays the status of the NTP client software on the switch. The status can be either enabled or disabled. If enabled, the switch seeks its date and time from the NTP server. The default is disabled.
Server	Displays the IP address of the NTP server. This value is set with “NTP PEER” on page 232.
UTC Offset	Displays the time difference, in hours and minutes, between UTC and local time. This value is set with “CLOCK TIMEZONE” on page 230.
Daylight Savings Time (DST)	Not supported.

Example

This example displays the settings of the NTP client:

```
awplus# show ntp associations
```

SHOW NTP STATUS

Syntax

```
show ntp status
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to determine whether or not the switch has synchronized its time with the specified NTP server. See Figure 43 for an example of the information.

```
Clock is synchronized, reference is 172.17.28.1
Clock offset is -07:00
```

Figure 43. SHOW NTP STATUS Command

The information is described here:

Table 38. SHOW NTP ASSOCIATIONS Command

Field	Description
Clock is	Indicates if the time on the switch is synchronized or unsynchronized with the NTP server.
Reference	Displays the IP address of the NTP server. This value is set with “NTP PEER” on page 232.
clock offset	Displays the specified time difference, in hours and minutes, between UTC and local time. This value is set with “CLOCK TIMEZONE” on page 230.

Example

This example displays information about an NTP server:

```
awplus# show ntp status
```

Section II

Layer 2 Switching

This section contains the following chapters:

Chapter 11

Port Parameter Commands

The port parameter commands are summarized in Table 39.

Table 39. Port Parameter Commands

Command	Mode	Description
“CLEAR PORT COUNTER” on page 241	User Exec and Privileged Exec	Clears the packet counters.
“CUT-THROUGH” on page 242	Port Interface	Changes the switch forwarding method to the cut-through switching method.
“DESCRIPTION” on page 243	Port Interface	Adds a port description.
“EGRESS-RATE-LIMIT” on page 244	Port Interface	Sets a limit on the amount of traffic that can be transmitted per second from the port.
“FLOWCONTROL RECEIVE” on page 245	Port Interface	Enables or disables flow control receive (Rx) on ports.
“INTERFACE” on page 249	Global Configuration	Moves from the Global Configuration mode to the Port Interface mode.
“MIRROR” on page 247	Port Interface	Specifies the port as the mirror port.
“NO DESCRIPTION” on page 251	Port Interface	Removes a port description.
“NO EGRESS-RATE-LIMIT” on page 252	Port Interface	Disables egress rate limiting on the ports.
“NO FLOWCONTROL” on page 253	Port Interface	Disables flow control receive (Rx) on ports.
“NO SHUTDOWN” on page 254	Port Interface	Activates ports that were disabled to resume forwarding network traffic again.
“NO STORM-CONTROL” on page 255	Port Interface	Removes threshold limits for broadcast, multicast, or unknown unicast packets.
“PURGE” on page 256	Port Interface	Restores the default settings.
“RESET” on page 257	Port Interface	Performs software resets on the ports.

Table 39. Port Parameter Commands (Continued)

Command	Mode	Description
“SHOW FLOWCONTROL INTERFACE” on page 258	Privileged Exec	Displays the current settings for flow control on the ports.
“SHOW INTERFACE” on page 260	Privileged Exec	Displays port settings.
“SHOW INTERFACE BRIEF” on page 263	Privileged Exec	Displays the link status of the ports.
“SHOW INTERFACE STATUS” on page 265	Privileged Exec	Displays the speed and duplex mode settings of the ports.
“SHOW MIRROR” on page 267	Privileged Exec	Displays the settings of mirror ports on the switch.
“SHOW PLATFORM PORT COUNTERS” on page 269	Privileged Exec	Displays packet statistics for the individual ports.
“SHOW PLATFORM PORT COUNTERS SUMMARY” on page 274	Privileged Exec	Displays summary statistics about packets for all the ports.
“SHOW STORM-CONTROL” on page 275	Privileged Exec	Displays the specified maximum limit of broadcast, multicast, or unknown unicast packets per a port.
“SHUTDOWN” on page 277	Port Interface	Disables ports to stop them from forwarding network traffic.
“STORM-CONTROL” on page 278	Port Interface	Sets a maximum limit of broadcast, multicast, or unknown unicast packets per a port.

CLEAR PORT COUNTER

Syntax

```
clear port counter port_ids
```

Parameter

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

User Exec mode

Description

Use this command to clear the packet counters on a port, or ports.

Confirmation Command

"SHOW PLATFORM PORT COUNTERS" on page 269

Example

This example clears the packet counters for ports 1.0.4 through 1.0.7:

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

CUT-THROUGH

Syntax

```
cut-through
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to change the switch forwarding method to cut-through switching on a port or ports. Two switch forwarding methods are available on each port: cut-through switching and store-and-forward switching. By default, all the ports are set with the store-and-forward switching method.

Use the NO CUT-THROUGH command to configure ports with the store-and-forward switching method.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Examples

This example changes the switch forwarding method to cut-through switching:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.20
awplus(config-if)# cut-through
```

This example changes the switching forwarding method to store-and forward switching:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.20
awplus(config-if)# no cut-through
```

DESCRIPTION

Syntax

```
description description
```

Parameter

description
: Specifies a description of 1 to 72 alphanumeric characters for a port. Spaces and special characters except exclamation marks (!) and question marks (?) are permitted.

Mode

Port Interface mode

Description

Use this command to add a description to a port on the switch or overwrite the existing description with a new description.

Confirmation Command

"SHOW INTERFACE" on page 260

Example

This example assigns the description "Connected to S2 on the 3rd floor" to port1.0.15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# description Connected to S2 on the 3rd
floor
```

EGRESS-RATE-LIMIT

Syntax

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

Parameter

value
: Specifies the maximum amount of traffic that can be transmitted from the port. The value is kilobits per second. The range is 1 to 40,000,000 kbps. The maximum rate for 10G ports is 10,000,000 kbps.

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. By default, the value is not specified.

When you specify a value, which is not an increment of 64, the switch rounds up the specified value to an increment of 64.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example sets the egress rate limit to 8,000 kilobits per second on port 1.0.13:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.13
awplus(config-if)# egress-rate-limit 8000
```

FLOWCONTROL RECEIVE

Syntax

```
flowcontrol receive on|off
```

Parameters

on
: Enables flow control.

off
: Disables flow control.

Mode

Port Interface mode

Description

Use this command to enable or disable flow control receive (Rx) on a port or ports. When flow control Rx is enabled, a port stops sending packets when the port receives PAUSE packets from a link partner. The switch supports flow control to respond to PAUSE packets when receiving them and does *not* support of flow control transmit (Tx) to transmit PAUSE packets.

To disable flow control Rx, specify the "off" keyword. The FLOWCONTROL RECEIVE OFF is equivalent to "NO FLOWCONTROL" on page 253.

Confirmation Command

"SHOW FLOWCONTROL INTERFACE" on page 258

Examples

This example configures ports 1.0.19 through 1.0.29 to respond to PAUSE packets from a link partner:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.19-port1.0.29
awplus(config-if)# flowcontrol receive on
```

This example configures ports 1.0.18 through 1.0.20 and port 1.0.24 to disable flow control Rx:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18-port1.0.20,port1.0.24
awplus(config-if)# flowcontrol receive off
```

MIRROR

Syntax

```
mirror [interface port_ids direction both|receive|transmit]
```

Parameters

port_ids
: Specifies a port ID or multiple port IDs of source ports. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

`both`
: Specifies both receiving and transmitting frames of source ports. The specified mirror port receives the copies of these frames.

`receive`
: Specifies receiving frames of source ports. The specified mirror port receives the copies of these frames.

`transmit`
: Specifies transmitting frames of source ports. The specified mirror port receives the copies of these frames.

Mode

Port Interface mode

Description

Use this command to specify a port as the mirror port. In addition, you can specify the direction of frames that the mirror port receives from the source port: receive, transmit, or both. The mirror port receive copies of receiving frames without VLAN tags and transmitting frames with VLAN tags. The switch does not copy and send PAUSE frames and broadcast packets that the switch generates.

When you specify the port as the mirror port for the copy-to-mirror action of hardware access control lists (ACLs) or policy maps, enter this command without any parameters. For information about ACLs, see Chapter 20, "ACL Commands" on page 443.

You can specify only one port as a mirror port for the switch. Once the port becomes a mirror port, the port does not belong to any VLAN.

To cancel the port as a mirror port, use the NO MIRROR command. The port restores the membership of the VLAN before the port was designated as a mirror port.

To remove a source port from a mirror port, use the NO MIRROR command.

Confirmation Command

"SHOW MIRROR" on page 267

Examples

This example specifies port 1.0.5 as the mirror port to receive copies of packets that port 1.0.8 receives and transmits:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.8 direction both
```

This example specifies port 1.0.5 as the mirror port to receive copies of packets that ports 1.0.2 and 1.0.4 receive:

```
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.2,port1.0.4
direction receive
```

This example removes port 1.0.4 as a source port:

```
awplus(config)# interface port1.0.1
awplus(config-if)# no mirror interface port1.0.4
```

This example uses a hardware ACL to copy only TCP packets that port 1.0.1 and 1.0.2 receive and send the copies to port 1.0.24:

```
awplus(config)# access-list hardware mirr_acl1
awplus(config-ip-hw-acl)# copy-to-mirror tcp any any
awplus(config-ip-hw-acl)# exit
awplus(config)# interface port1.0.1-1.0.2
awplus(cofig-if)# access-group mirr_acl1
awplus(cofig-if)# exit
awplus(config)# interface port1.0.24
awplus(config-if)# mirror
```

This example cancels port 1.0.24 as the mirror port:

```
awplus(config)# interface port1.0.24
awplus(config-if)# no mirror
```

INTERFACE

Syntax

`interface` *port_ids*|sa*X*|po*X*|`eth0`

Parameters

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

sa*X*
: Specifies a static port trunk ID or multiple static port trunk IDs where X indicates the number of the port trunk ID. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

po*X*
: Specifies a dynamic port trunk ID or multiple dynamic port trunk IDs where X indicates the number of the port trunk ID. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

eth0
: Specifies the management Ethernet port.

Mode

Global Configuration mode

Description

Use this command to move from the Global Configuration mode to the Port Interface mode to configure ports. When configuring dynamic and static trunk groups, specify this command with the saX or poX parameter.

Examples

This example moves to the Port Interface mode to configure ports 1.0.1 through 1.0.10:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-1.0.10
```

This example moves to the Port Interface mode to configure the static port trunk sa1:

```
awplus# configure terminal
awplus(config)# interface sa1
```

NO DESCRIPTION

Syntax

```
no description
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove a description from a switch port.

Confirmation Command

"SHOW INTERFACE" on page 260

Example

This example removes the current description from port1.0.15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# no description
```

NO EGRESS-RATE-LIMIT

Syntax

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

Parameters

None

Mode

Port Interface mode

Description

Use this command to delete egress rate limit on the ports.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example deletes egress rate limit on ports 1.0.4 and 1.0.5:

```
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
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable flow control on ports to respond to receive PAUSE packets.

This command is equivalent to the FLOWCONTROL RECEIVE OFF command. See "FLOWCONTROL RECEIVE" on page 245.

Confirmation Command

"SHOW FLOWCONTROL INTERFACE" on page 258

Example

This example disables flow control on ports 1.0.20 through port 1.0.24:

```
awplus(config)# interface port1.0.20,port1.0.24
awplus(config-if)# no flowcontrol
```

NO SHUTDOWN

Syntax

```
no shutdown
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to enable ports to forward packets.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example enables port 1.0.22:

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

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 the STORM-CONTROL command. See "STORM-CONTROL" on page 278.

Confirmation Command

"SHOW STORM-CONTROL" on page 275

Examples

This example removes the threshold limit for broadcast packets on port 1.0.12:

```
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 1.0.5:

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

PURGE

Syntax

```
purge
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to restore the default settings configured with the following commands:

- ❒ “CUT-THROUGH” on page 242
- ❒ “DESCRIPTION” on page 243
- ❒ “EGRESS-RATE-LIMIT” on page 244
- ❒ “FLOWCONTROL RECEIVE” on page 245
- ❒ “SHUTDOWN” on page 277
- ❒ “SNMP TRAP LINK-STATUS” on page 214
- ❒ “STORM-CONTROL” on page 278

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116, “SHOW INTERFACE” on page 260, “SHOW FLOWCONTROL INTERFACE” on page 258, “SHOW INTERFACE STATUS” on page 265, and “SHOW STORM-CONTROL” on page 275

Example

This example restores the default settings to ports 1.0.5, 1.0.6 and 1.0.12:

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

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. You may want to reset a port if it is experiencing a problem.

Example

This example resets port 1.0.14:

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

SHOW FLOWCONTROL INTERFACE

Syntax

```
show flowcontrol interface port_ids
```

Parameter

port_ids
Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Modes

Privileged Exec mode

Description

Use this command to display the current settings for flow control on the ports. The switch supports flow control to suspend packets from forwarding when receiving PAUSE packets and does not support flow control to transmit PAUSE packets. See Figure 44 for an example of the information.

```
Port     Send     Receive     RxPause     TxPause
         admin    admin
-----    -------  -------     -------     -------
1.0.13   no       yes         0           0
```

Figure 44. SHOW FLOWCONTROL INTERFACE Command

The fields are described in Table 40.

Table 40. SHOW FLOWCONTROL INTERFACE Command

Parameter	Description
Port	Indicates the port ID.
Send admin	Not supported.
Receive admin	Indicates flow control is enabled (yes) or disabled (no).
RxPause	Indicates the number of received PAUSE packets.
TxPause	Not supported.

Example

This command displays the flow control settings for port 1.0.2:

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

SHOW INTERFACE

Syntax

`show interface [`*`port_ids`*`|sa`*`X`*`|po`*`X`*`|eth0]`

Parameters

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

sa*X*
: Specifies a static port trunk ID or multiple static port trunk IDs where X indicates the number of the port trunk ID. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

po*X*
: Specifies a dynamic port trunk ID or multiple dynamic port trunk IDs where X indicates the number of the port trunk ID. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

eth0
: Specifies the management Ethernet port.

Modes

Privileged Exec mode

Description

Use this command to display information about the ports. When you do not specify a port interface, the switch displays information about all the switch ports and the management port. See Figure 45 on page 261 for an example of the information.

```
Interface port1.0.1
   Link is UP, administrative state is UP
   Address is 0014.7700.0001
   Description:
   index 1 mtu 12288
   current duplex full, current speed 10G, polarity auto, flowcontrol disabled
   configured duplex full, configured speed 10000
Unknown Ingress Multicast Blocking: Disabled
Unknown Egress Multicast Blocking: Disabled
   SNMP link-status traps: Disabled (Suppressed in 0 sec.)
   input packets 0, bytes 0, dropped 0, multicast packets 0
   output packets 15, bytes 2880, multicast packets 45 broadcast packets 0

Interface port1.0.2
   Link is UP, administrative state is UP
   Address is 0014.7700.0002
   Description:
   index 2 mtu 12288
   current duplex full, current speed 10G, polarity auto, flowcontrol disabled
   configured duplex full, configured speed 10000
Unknown Ingress Multicast Blocking: Disabled
Unknown Egress Multicast Blocking: Disabled
   SNMP link-status traps: Disabled (Suppressed in 0 sec.)
   input packets 0, bytes 0, dropped 0, multicast packets 0
   output packets 55, bytes 3520, multicast packets 55broadcast packets 0
```

Figure 45. SHOW INTERFACE Command

The fields are described in Table 41.

Table 41. SHOW INTERFACE Command

Field	Description
Interface	Indicates the port number.
Link is	Indicates the link status of the port.
administrative state is	Indicates the administrative state of the port. The administrative state is DOWN if the port was disabled with the SHUTDOWN command.
Address is	Displays the MAC address of the port.
Description	Displays the port's description. To set the description, refer to "DESCRIPTION" on page 243.
Index	Displays the index number of the port. This field is only for the switch ports.

Table 41. SHOW INTERFACE Command (Continued)

Field	Description
mtu	Indicates the maximum frame size that the switch port can send and receive. For the management port (eth0), it indicates the maximum packet size that the management port can send and receive.
current duplex	Displays the current duplex mode when an SFP+/QSFP+ module is connected.
current speed	Displays the current speed when an SFP+/ QSFP+ module is connected.
polarity	Displays the wiring configuration when an SFP+/ QSFP+ module is connected.
flowcontrol	Displays the state of flow control. This field is only for the switch ports.
configured duplex	Displays the configured duplex mode when an SFP+/QSFP+ module is connected.
configured speed	Displays the configured speed when an SFP+/ QSFP+ module is connected.
Unknown Ingress/ Multicast Blocking	Not supported.
Unknown Egress/ Multicast Blocking	Not supported.
SNMP link-status traps	Displays the status of SNMP link traps on the port. The options are: ❒ Enabled: The port transmits SNMP notifications. ❒ Disabled: The port does not transmit SNMP notifications.
input packets	Displays the numbers of packets received by the port.
output packets	Displays the numbers of packets that the port transmits.

Example

This command displays the current operational state of ports 1.0.1 to 1.0.4:

```
awplus# show interface port1.0.1-1.0.4
```

SHOW INTERFACE BRIEF

Syntax

```
show interface [port_ids|saX|poX|eth0] brief
```

Parameters

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

sa*X*
: Specifies a static port trunk ID or multiple static port trunk IDs where X indicates the number of the port trunk ID. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

po*X*
: Specifies a dynamic port trunk ID or multiple dynamic port trunk IDs where X indicates the number of the port trunk ID. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

eth0
: Specifies the management Ethernet port.

Modes

Privileged Exec mode

Description

Use this command to display the link status of the ports. When you do not specify a port interface, the switch displays the link status of all the switch ports and the management port. See Figure 46 for an example.

```
Interface     Status    Protocol
port1.0.1    admin up      up
port1.0.2    admin up      up
port1.0.3    admin up      up
.....
port1.0.49   admin up     down
port1.0.53   admin up     down
port1.0.57   admin up     down
port1.0.61   admin up     down
eth0         admin up      up
```

Figure 46. SHOW INTERFACE BRIEF Command

The fields are described in Table 41.

Table 42. SHOW INTERFACE 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.
Protocol	Indicates the link status of the port.

Example

This command displays the link status of ports 1.0.1 to 1.0.20:

```
awplus# show interface port1.0.1-1.0.20 brief
```

SHOW INTERFACE STATUS

Syntax

```
show interface [port_ids|eth0] status
```

Parameters

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

eth0
: Specifies to display the management Ethernet port.

Modes

Privileged Exec mode

Description

Use this command to display the link status, VLAN settings, duplex mode, speed, and connected media type of the specified ports. When you do not specify port IDs or eth0, the switch displays the statuses of the all the ports. See Figure 47 for an example of the information.

```
Port       Name   Status       Vlan   Duplex  Speed   Type

port1.0.1         connected      1    full    10G     10GBASE-SR

port1.0.2         connected      1    full    10G     10GBASE-SR

port1.0.3         not connect    1    full    10G     not present

....

port1.0.49        not connect    1    full    40G     not present

port1.0.53        not connect    1    full    40G     not present

port1.0.57        not connect    1    full    40G     not present

port1.0.61        not connect    1    full    40G     not present

eth0              connected    none   a-half  a-10    1000Base-T
```

Figure 47. SHOW PLATFORM PORT COUNTERS

The fields are described in Table 43.

Table 43. SHOW INTERFACE STATUS Command

Field	Description
Port	Displays the port ID.
Name	Displays the description of the port. To set the description, refer to “DESCRIPTION” on page 243.
Status	Displays the link status of the port. The options are: ❒ connected: link up ❒ not connect: link down ❒ disabled: shutdown
VLAN	Displays the ID of the VLAN when the port is an untagged member. If the port is a tagged port, “trunk” is displayed.
Duplex	Displays the duplex mode. When the port status is “connected,” the switch displays the current duplex mode of the port. The prefix “a-” means that the duplex mode is set with Auto-negotiation. When the port status is “not connect” or “disabled,” the switch displays the duplex mode setting of the port.
Speed	Displays the speed. When the port status is “connected,” the switch displays the current speed of the port. The prefix “a-” means that the speed is set with Auto-negotiation. When the port status is “not connect” or “disabled,” the switch displays the speed setting of the port.
Type	Displays the media type of the module connected to the port interface. When SFP+ and QSFP+ ports do not recognize the module, the switch displays “Unknown.” When no module is connected or the connected module is not working, the switch displays “not present.”

Examples

This command displays the settings of all the ports:

```
awplus# show interface status
```

This command displays the settings of port 1.0.17, port 1.0.18, and the management port:

```
awplus# show interface port1.0.17,1.0.18 status
```

SHOW MIRROR

Syntax

```
show mirror
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the settings of the mirror port on the switch. See Figure 48 for an example.

```
Mirror Test Port Name: port1.0.40
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.41
Mirror Test Port Name: port1.0.40
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.42
Mirror Test Port Name: port1.0.40
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.43
Mirror Test Port Name: port1.0.40
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.44
```

Figure 48. SHOW MIRROR

The fields are described in Table 44.

Table 44. SHOW MIRROR Command

Field	Description
Mirror Test Port Name	Displays the port ID of the mirror port.
Mirror option	Indicates that Port Mirroring is enabled or disabled.

Table 44. SHOW MIRROR Command (Continued)

Field	Description
Mirror direction	Indicates the direction of the traffic on the source port that the switch copies.
Monitored Port Name	Indicates the port ID of the source port.

Example

This command displays the settings of the mirror port on the switch:

```
awplus# show mirror
```

SHOW PLATFORM PORT COUNTERS

Syntax

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

show platform table port counters summary
```

Parameter

port-ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

Privileged Exec mode

Description

Use this command to display packet statistics for the individual ports on the switch for troubleshooting. If you do not specify a port ID, the command displays the statistics for all of the ports. See Figure 49 on page 270 for an example of the command output.

```
 Switch Port Counters
-------------------------------------------------------------

Port port1.0.14 Ethernet MAC counters:
 Combined receive/transmit packets by size (octets) counters:
  64                   458   1024-MaxPktSz                76
  65-127               236   1519-1522                     -
  128-255               98   1519-2047                    23
  256-511               59   2048-4095                     0
  512-1023             130   4096-9216                     0

 General counters:
 Receive                     Transmit
  Octets            291024   Octets                    41144
  Pkts                 993   Pkts                         87
  CRCErrors              0
  FCSErrors              0
  MulitcastPkts        491   MulticastPkts                51
  BroadcastPkts         64   BroadcastPkts                 1
  PauseMACCtlFrms        0   PauseMACCtlFrms               0
  OversizePkts          23
  Fragments                  0
  Jabbers                    0
  UnsupportOpcode            0
  AlignmentErrors            0
  CarrierSenseErr            0
  UndersizePkts              0
                             FrameWDeferrdTx               0
                             SingleCollsnFrm               0
                             MultCollsnFrm                 0
                             LateCollisions                0
                             ExcessivCollsns               0
                             Collisions                    0

Layer 3 Counters:
  ifInUcastPkts        438   ifOutUcastPkts               35
  ifInDiscards         438   ifOutErrors                   0
  ipInHdrErrors          0

Miscellaneous counters:
  MAC RxErr              0   MAC TxErr                     0
  Drop Events          438
  ifOutDiscards          0
  MTUExcdDiscard         0

-------------------------------------------------------------
```

Figure 49. SHOW PLATFORM PORT COUNTERS

The fields are described in Table 45 on page 271.

Table 45. SHOW PLATFORM PORT COUNTERS Command

Parameter	Description
Combined receive/transmit packets by size (octets) counters:	
64 65- 1 27 128 - 255 256 - 511 512 - 1023 1024 - MaxPktSz 1519 - 1522 1519 - 2047 2048 - 4095 4096 - 9216	Displays the numbers of frames transmitted and received by the port, grouped by frame size.
General counters: Receive	
Octets	Displays the number of received octets.
Pkts	Displays the number received packets.
CRCErrors	Displays the number of ingress frames with a Cyclic Redundancy Check (CRC) error.
FCSErrors	Displays the number of ingress frames that had Frame Check Sequence (FCS) errors.
MulticastPkts	Displays the number of received multicast frames.
BroadcastPkts	Displays the number of received broadcast frames.
PauseMACCtlFrms	Displays the number of received PAUSE packets when flow control is enabled.
OversizePkts	Displays the number of received frames that exceeded the maximum size (1518 octets).
Fragments	Displays the number of ingress undersized frames, which are less than 64 octets and have FCS errors, including alignment errors.
Jabbers	Displays the number of ingress jabber frames, which are larger than 1518 octets and have FCS errors, including alignment errors.
UnsupportOpcode	Displays the number of unsupported MAC Control frames (MAC Control frames except PAUSE frames).

Table 45. SHOW PLATFORM PORT COUNTERS Command (Continued)

Parameter	Description
AlignmentErrors	Displays the number of received frames with alignment errors. A frame with an alignment error is a frame whose length is not an increment of 8 bits.
CarrierSenseErr	Displays the number of carrier sense errors detected between frames.
UndersizePkts	Displays the number of frames that are less than 64 octets.
General counters: Transmit	
Octets	Displays the number of transmitted octets.
Pkts	Displays the number transmitted packets.
MulticastPkts	Displays the number of transmitted multicast frames.
BroadcastPkts	Displays the number of transmitted broadcast frames.
PauseMACCtrlFrms	Displays the number of transmitted PAUSE packets.
FrameWDeferrdTx	Displays the number of frames that were transmitted successfully without causing any collisions after their transmissions were delayed due to carrier sense detection.
SingleCollsnFrm	Displays the number of frames that caused one collision.
MultCollsnFrm	Displays the number of frames that caused more than one collision.
LateCollisions	Displays the number of frames that caused late collisions.
ExcessivCollsns	Displays the number of frames that transmission was cancelled due to excessive collisions.
Collisions	Displays the total number of collisions on the port.
Layer 3 Counters	
ifInUcastPkts	Displays the number of unicast packets that were received in the Layer 3 interface.

Table 45. SHOW PLATFORM PORT COUNTERS Command (Continued)

Parameter	Description
ifInDiscards	Displays the number of discarded packets that were received in the Layer 3 interface.
ipInHdrErrors	Displays the number of discarded packets because of an IP header error.
ifOutUcastPkts	Displays the number of unicast packets that were transmitted from the Layer 3 interface.
ifOutErrors	Displays the number of packets that were discarded before being transmitted from the Layer 3 interface.
Miscellaneous Counters	
MAC RxErr	Displays the number of frames that failed to be received due to a MAC address error.
Drop Events	Displays the number of packets received but were discarded.
ifOutDiscards	Displays the number of packets discarded prior to transmission.
MTUExcdDiscard	Displays the number of packets that exceed the specified MTU value.
MAC TxErr	Displays the number of frames that failed to be transmitted due to a MAC address error.

Examples

This command displays the statistics for ports 1.0.21 and 1.0.23:

```
awplus# show platform 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 PLATFORM PORT COUNTERS SUMMARY

Syntax

```
show platform table port counters summary
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display summary statistics on packets that all the ports on the switch transmitted and received. To view packet statistics for individual ports, see “SHOW PLATFORM PORT COUNTERS” on page 269.

The fields are described in Table 45 on page 271.

Example

This command displays the summary statistics on ingress and egress packets on the switch:

```
awplus# show platform port counters summary
```

SHOW STORM-CONTROL

Syntax

```
show storm-control [port_ids]
```

Parameter

port-ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Modes

Privileged Exec mode

Description

Use this command to display the current settings of storm control. The command displays the specified maximum number of broadcast, multicast, and unknown unicast packets per second. See Figure 50 for an example of the information.

```
Port       BcastLevel       McastLevel       Dlflevel
Port1.0.1     3000000          5000000       7000000
Port1.0.2     3000000          5000000       7000000
Port1.0.3     3000000          5000000       7000000

....
```

Figure 50. SHOW STORM-CONTROL Command

The fields are described in Table 46.

Table 46. SHOW STORM-CONTROL Command

Field	Description
Port	Indicates the port ID.
BcastLevel	Indicates the specified maximum number of ingress broadcast packets per second.
McastLevel	Indicates the specified maximum number of ingress multicast packets per second.
DifLevel	Indicates the specified maximum number of ingress multicast packets per second.

Example

This command displays the storm control settings for port 1.0.2:

```
awplus# show storm-control port1.0.2
```

SHUTDOWN

Syntax

```
shutdown
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable ports. When you disable a port, the port status changes to the link-down state and the port does not forward traffic. You may want to disable unused ports to secure them from unauthorized use. In addition, you want to disable ports 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 254.

Confirmation Command

"SHOW INTERFACE" on page 260

Example

This example disables ports 1.0.15 and 1.0.16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15,port1.0.16
awplus(config-if)# shutdown
```

STORM-CONTROL

Syntax

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

Parameters

`broadcast`
Specifies broadcast packets.

`multicast`
Specifies multicast packets.

`dlf`
Specifies unknown unicast packets.

`value`
Specifies the maximum number of ingress packets per second of the specified packet type. Units are packets per second (pps), Kpps, and Mpps. Specify one of the following formats:

- 1 to 33554368: Specify a number in this range. The unit is pps. The maximum number for 10G ports is 14,880,900.
- 1k to 3276k: Specify a number in this range with “k” as the suffix. The unit is Kpps. The suffix “k” is not case-sensitive. The maximum number for 10G ports is 14,532K.
- 1m to 31m: Specify a number in this range with “m” as the suffix. The unit is Mpps. The suffix “m” is not case-sensitive. The maximum number for 10G ports is 14M.

Mode

Port Interface mode

Description

Use this command to set thresholds for the ingress packets on the ports. Ingress packets that exceed the thresholds are discarded by the ports. You can set thresholds independently for broadcast packets, multicast packets, and unknown unicast packets.

Confirmation Command

“SHOW STORM-CONTROL” on page 275

Examples

This example sets the maximum threshold level of 5,000 pps for ingress broadcast packets on port 1.0.12:

```
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 pps for ingress multicast packets on port 1.0.4:

```
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 pps for ingress unknown unicast packets on ports 1.0.15 and 1.0.17:

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

Chapter 12

LACP Commands

The LACP port trunk commands are summarized in Table 47.

Table 47. LACP Port Trunk Commands

Command	Mode	Description
“CHANNEL-GROUP” on page 282	Port Interface	Creates a new dynamic LACP trunk group and adds ports to an existing dynamic trunk group.
“LACP SYSTEM-PRIORITY” on page 284	Global Configuration	Sets the LACP system priority value for the switch.
“NO CHANNEL-GROUP” on page 285	Port Interface	Removes ports from the LACP trunk group and deletes the trunk group.
“PORT-CHANNEL LOAD-BALANCE” on page 286	Port Interface	Sets the load distribution method to a trunk group.
“SHOW ETHERCHANNEL” on page 288	Privileged Exec	Displays information about trunk groups and LACP trunk groups on the switch.
“SHOW ETHERCHANNEL DETAIL” on page 290	Privileged Exec	Displays detailed information about the LACP trunk groups on the switch
“SHOW ETHERCHANNEL SUMMARY” on page 293	Privileged Exec	Displays the states of the member ports of the LACP trunk groups.
“SHOW LACP SYS-ID” on page 295	Privileged Exec	Displays the LACP priority value and MAC address of the switch.
“SHOW PORT ETHERCHANNEL” on page 296	Privileged Exec	Displays the LACP port information.
“SHOW STATIC-CHANNEL-GROUP” on page 300	Privileged Exec	Displays information about static trunk groups on the switch.
“STATIC-CHANNEL-GROUP” on page 302	Port Interface	Creates a new static trunk group and adds ports to an existing static trunk group.

CHANNEL-GROUP

Syntax

```
channel-group id_number
```

Parameter

id_number
: Specifies the ID number of a new or an existing LACP trunk group. The range is from 1 to 65,335.

Mode

Port Interface mode

Description

Use this command to create a new LACP trunk group (dynamic trunk group) or to add ports to existing LACP channel group. You can create up to 32 trunk groups on the switch, including the dynamic LACP and static trunk groups.

To create a new LACP trunk group or add ports to an existing LACP trunk group, the member ports must belong to the same VLAN and have the same switchport mode: either access or trunk.

The lowest numbered port in an LACP trunk group is called the *base port*. When adding ports to an existing LACP trunk group, you cannot add ports that are below the base port. For example, you cannot add ports 1.0.1 to 1.0.6 to an existing LACP trunk group that consists of ports 1.0.7 to 1.0.12. Instead, you must delete and recreate a trunk group to change its base port.

Confirmation Command

“SHOW ETHERCHANNEL” on page 288

Examples

This example creates a new LACP trunk group consisting of ports 1.0.11 through 1.0.16. The ID number of the LACP trunk group 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 1.0.15 to an existing LACP trunk group that has the ID number 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# channel-group 2
```

LACP SYSTEM-PRIORITY

Syntax

```
lacp system-priority priority
```

Parameter

priority
: Specifies the LACP system priority value for the switch. The range is 1 to 65,535. By default, the priority value for the switch is 32,768. The value of 1 has the highest priority.

Mode

Global Configuration mode

Description

Use this command to change the LACP priority of the switch. The switch uses the LACP priority to resolve conflicts with other network devices when the switch creates LACP trunk groups. The settings on the device with the higher priority takes precedence over the settings on the partner device. If both devices have the same LACP system priority value, the settings on a device that has the lower MAC address takes precedence.

To set the LACP system priority value to the default value of 32,768, use the NO LACP SYSTEM-PRIORITY command.

Confirmation Command

“SHOW LACP SYS-ID” on page 295

Example

This example assigns a system priority of 200 to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# lacp system-priority 200
```

NO CHANNEL-GROUP

Syntax

```
no channel-group
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to remove ports from an LACP trunk group and to delete the LACP trunk group. To delete an LACP trunk group, remove all the member ports.

You cannot remove the base port of the LACP trunk group. If you want to change the base port, you must delete and recreate the LACP trunk group.

Confirmation Command

"SHOW ETHERCHANNEL" on page 288

Example

This example deletes ports 1.0.11 and 1.0.12 from an LACP trunk group. The LACP trunk group is deleted if ports 1.0.11 and 1.0.12 are the only member ports of the trunk group:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.12
awplus(config-if)# no 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 both the source address and the destination MAC address.

`src-ip`
Specifies source IP address.

`dst-ip`
Specifies destination IP address.

`src-dst-ip`
Specifies both the source address and the destination IP address.

Mode

Port Interface mode

Description

Use this command to set the load distribution methods of a trunk group. A trunk group can have only one load distribution method.

This command can be applied only to dynamic LACP and static trunk groups. To enter the Port Interface mode for a specific trunk group, enter the INTERFACE command with the ID number of the trunk group.

Confirmation Command

“SHOW ETHERCHANNEL DETAIL” on page 290

Example

This example sets the load distribution method to the source MAC address for the LACP trunk group that has an ID number of 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
```

Parameter

id_number
Specifies the ID number of an LACP trunk group.

Mode

Privileged Exec mode

Description

Use this command to display information about trunk groups and the specific LACP trunk group on the switch. When you do not specify the ID number of an LACP trunk group, the command displays information about trunk groups and all the LACP trunk groups on the switch. See Figure 51 for an example of the command output.

```
% LAG Maximum            :32
% LAG Static Maximum     :32
% LAG Dynamic Maximum    :32
% LAG Static Count       :3
% LAG Dynamic Count      :2
% LAG Total Count        :5
% LAG Aggregator         :po2
% Load-Balancing         :MACBoth
% Member:
%    port1.0.13
%    port1.0.14
% LAG Aggregator:         po1
% Load-Balancing:         MACBoth
% Member:
%    port1.0.25
%    port1.0.26
%    port1.0.27
%    port1.0.28
```

Figure 51. SHOW ETHERCHANNEL Command

The fields are described in Table 48.

Table 48. SHOW ETHERCHANNEL Command

Field	Description
LAG Maximum	Indicates the maximum number of dynamic LACP and static trunk groups that the switch can have.
LAG Static Maximum	Indicates the maximum number of static trunk groups that the switch can generate.
LAG Dynamic Maximum	Indicates the maximum number of dynamic LACP trunk groups that the switch can generate.
LAG Static Count	Indicates the number of static trunk groups on the switch.
LAG Dynamic Count	Indicates the number of dynamic LACP trunk groups on the switch.
LAG Total Count	Indicates the number of static and dynamic LACP trunk groups on the switch.
LAG Aggregator	Displays the ID number of an LACP trunk group.
Load-Balancing	Displays the load balance settings of the LACP trunk group. The options are: ❒ MACSrc: Source MAC address ❒ MACDest: Destination MAC address ❒ MACBoth: Source and Destination MAC addresses ❒ IPSrc: Source IP address ❒ IPDest: Destination IP address ❒ IPBoth: Source and Destination IP addresses
Member	Lists the member ports of the LACP trunk group.

Example

This example displays information about trunk groups as well as the LACP trunk group with an ID number of 22:

```
awplus# show etherchannel 22
```

SHOW ETHERCHANNEL DETAIL

Syntax

```
show etherchannel detail
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display detailed information about the LACP trunk groups on the switch. See Figure 52 for an example of the output.

```
Aggregator # 2..... po2
Mac address: (00-E0-0C-02-01-FD,FF0D)
Admin Key: 0xff0d - Oper Key: 0x0d0d
Receive link count: 2 - Transmit link count: 2
Individual: 0 - Ready: 0
Distribution Mode .. MACBoth
Partner LAG: (8000,00-15-77-FF-00-02,FF0D)
  Link: Port 1.0.13    sync
  Link: Port 1.0.14    sync

Aggregator # 1..... po1
Mac address: (00-E0-0C-02-01-FD,FF19)
Admin Key: 0xff19 - Oper Key: 0x1919
Receive link count: 1 - Transmit link count: 1
Individual: 0 - Ready: 0
Distribution Mode .. MACBoth
Partner LAG: (8000,00-15-77-FF-00-02,FF19)
Link: Port 1.0.25disabled
  Link: Port 1.0.26    sync
  Link: Port 1.0.27    disabled
  Link: Port 1.0.28    disabled
```

Figure 52. SHOW ETHERCHANNEL DETAIL Command

The fields are described in Table 49.

Table 49. SHOW ETHERCHANNEL SUMMARY Command

Field	Description
Aggregator	Indicates the ID number of the LACP trunk group.
Mac address	Displays the MAC address of the switch and the Admin Key.
Admin Key	Indicates the value that is used to generate the LACP port key.
Oper Key	Indicates the LACP port key.
Receive link count	Displays the number of the member ports that have the link status of "wait" or "sync."
Transmit link count	Displays the number of the member ports that have the link status of "sync."
Individual	Indicates the aggregation flag. The options are: ❒ 0 - Aggregatable: The port can form an aggregation with other ports. ❒ 1 - Individual: The port does not have other ports to form an aggregation.
Ready	Indicates if the section logic is executable. ❒ 0 - Not Executable: The section logic is not executable. ❒ 1 - Executable: The section logic is executable.
Distribution Mode	Displays the load balance settings of the LACP trunk group. The options are: ❒ MACSrc: Source MAC address ❒ MACDest: Destination MAC address ❒ MACBoth: Source and Destination MAC addresses ❒ IPSrc: Source IP address ❒ IPDest: Destination IP address ❒ IPBoth: Source and Destination IP addresses
Partner LAG	Displays the MAC address and Admin Key of the other (partner) LACP device.

Table 49. SHOW ETHERCHANNEL SUMMARY Command (Continued)

Field	Description
Link	Indicates the status of the member port. The options are: ❒ sync: Active LACP member port ❒ wait: Standby port ❒ disabled: Port whose link is down

Example

This example displays detailed information about the LACP trunk groups on the switch:

```
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 LACP trunk groups. See Figure 53 for an example of the command output.

```
Aggregator # 2 .... po2
Admin Key: 0xff0d - Oper Key: 0x0d0d
    Link: Port1.0.13   sync
    Link: Port1.0.14   sync

Aggregator # 1 .... po1
Admin Key: 0xff19 - Oper Key: 0x1919
    Link: Port1.0.25   disabled
    Link: Port1.0.26   sync
    Link: Port1.0.27   disabled
    Link: Port1.0.28   disabled
```

Figure 53. SHOW ETHERCHANNEL SUMMARY Command

The fields are described in Table 50.

Table 50. SHOW ETHERCHANNEL SUMMARY Command

Field	Description
Aggregator	Indicates the ID number of the trunk group.
Admin Key	Indicates the value that is used to generate the LACP port key.
Oper Key	Indicates the LACP port key.

Table 50. SHOW ETHERCHANNEL SUMMARY Command (Continued)

Field	Description
Link	Indicates the status of the member port. The options are: ❒ sync: Indicates an active LACP member port ❒ wait: Indicates a standby port ❒ disabled: Indicates a port whose link is down

Example

This example displays the states of the member ports of the LACP trunk groups:

```
awplus# show etherchannel summary
```

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. See Figure 54 for an example of the command output.

```
System Priority: 0x0080 (32768)
Mac Address: 00-E0-0C-02-10-FD
```

Figure 54. SHOW LACP SYS-ID Command

The fields are described in Table 51.

Table 51. SHOW LACP SYS-ID Command

Field	Description
System Priority	Displays the LACP system priority of the switch. The value is displayed as both a hexadecimal and an integer.
MAC Address	DIsplays the MAC address of the switch.

Example

This example displays the LACP priority value and MAC address of the switch:

```
awplus# show lacp sys-id
```

SHOW PORT ETHERCHANNEL

Syntax

```
show port etherchannel port_ids
```

Parameter

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

Privileged Exec mode

Description

Use this command to display the LACP port information of the specified ports. See Figure 55 for an example of the command output.

```
Link: Port: 1.0.26

Aggregator # 1
Receive machine state: Current
Periodic Transmission machine state: Slow periodic
Mux machine state: Distributing
ACTOR                                PARTNER
================================================================================
Actor Port ............ 05          Partner Port ........ 26
Selected .............. SELECTED    Partner System ...... 00-15-77-FF-00-02
Oper Key .............. 0xff19      Oper Key  ........... 0xff19
Oper Port Priority ... 0x001a       Oper Port Priority .. 0x001a
Individual ............ NO          Individual .......... NO
Synchronized........... YES         Synchronized......... YES
Collecting  ........... YES         Collecting .......... YES
Distributing .......... YES         Distributing ........ YES
Defaulted ............. NO          Defaulted ........... NO
Expired ............... NO          Expired ............. NO
Actor Churn   ......... YES         Partner Churn ....... YES
```

Figure 55. SHOW PORT ETHERCHANNEL Command

The fields are described in Table 52.

Table 52. SHOW PORT ETHERCHANNEL Command

Field	Description
Port	Displays the Port ID.
Aggregator #	Displays the ID number of an LACP trunk group.
Receive machine state	Displays the state of the receive machine. The options are: ❒ Initialize ❒ Port-disabled ❒ Expired ❒ LACP-disabled ❒ Defaulted ❒ Current Refer to the IEEE 802.3ad standard for definitions of these options.
Periodic Transmission machine state	Displays the state of the periodic transmission machine. The options are: ❒ Fast periodic ❒ Slow periodic ❒ Periodic Tx Refer to the IEEE 802.3ad standard for definitions of the options.
Mux machine state	Displays the state of the MUX machine. The options are: ❒ Detached ❒ Waiting ❒ Attached ❒ Collecting ❒ Distributing Refer to the IEEE 802.3ad standard for definitions of these options.
Actor Port	Displays the port ID on the switch.
Partner Port	Displays the port ID of the partner device.

Table 52. SHOW PORT ETHERCHANNEL Command (Continued)

Field	Description
Selected	Displays the state of the port as an LACP member port. The options are: ❒ SELECTED: Active port ❒ STANDBY ❒ UNSELECTED: Disabled
Partner System	Displays the LACP system ID (MAC address) of the partner device.
Oper Key	Displays the LACP port key.
Oper Port Priority	Displays the LACP port priority.
Individual	Indicates the aggregation flag. The options are: ❒ Yes- Individual: The port does not have other ports to form an aggregation. ❒ No - Aggregatable: The port can form an aggregation with other ports.
Synchronized	Indicates the synchronization flag. The options are: ❒ YES - IN_SYNC ❒ NO - OUT_OF_SYNC
Collecting	Indicates the collecting flag. The options are: ❒ YES - Able to receive packets ❒ NO - Unable to receive packets
Distributing	Indicates the distributing flag. The options are: ❒ YES - Able to receive packets ❒ NO - Unable to receive packets
Defaulted	Indicates the defaulted flag. The options are: ❒ YES - Using default values for the partner device because the switch does not receive any LACP packets. ❒ NO - Using values from LACP packets
Expired	Indicates the expired flag. The options are: ❒ YES - The receive machine is expired. ❒ NO - The receive machine is not expired.

Table 52. SHOW PORT ETHERCHANNEL Command (Continued)

Field	Description
Actor Churn	Indicates if the port on the switch is detected as a churn. The churn is detected when the synchronization of the port is not stable and the port loses the active port status for a certain period of time. The options are: ❒ YES - A churn is detected. ❒ NO - A churn is not detected.
Partner Churn	Indicates if the port on the partner device is detected as a churn. The options are: ❒ YES - A churn is detected. ❒ NO - A churn is not detected.

Example

This example displays the LACP port information for port 1.0.26:

```
awplus# show port etherchannel port1.0.26
```

SHOW STATIC-CHANNEL-GROUP

Syntax

```
show static-channel-group
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display information about static trunk groups on the switch. See Figure 56 for an example of the command output.

```
% Static Aggregator:  : sa1
% Load-Balancing      : IPBoth
% Member:
    port1.0.1
    port1.0.2
    port1.0.3
    port1.0.4
% Static Aggregator   : sa2
% Load-Balancing      : MACBoth
% Member
    port1.0.5
    port1.0.6
    port1.0.7
    port1.0.8
% Static Aggregator   : sa3
% Load-Balancing      : MACBoth
% Member:
    port1.0.9
    port1.0.10
    port1.0.11
    port1.0.12
    port1.0.13
    port1.0.14
    port1.0.15
    port1.0.16
```

Figure 56. SHOW STATIC-CHANNEL-GROUP Command

The fields are described in Table 53.

Table 53. SHOW STATIC-CHANNEL-GROUP Command

Field	Description
Static Aggregator	Indicates the ID number of the static trunk group.
Load-Balancing	Displays the load balance settings of static trunk group. The options are: ❒ MACSrc: Indicates the source MAC address ❒ MACDest: Indicates the destination MAC address ❒ MACBoth: Indicates both the source and destination MAC addresses ❒ IPSrc: Indicates the source IP address ❒ IPDest: Indicates the destination IP address ❒ IPBoth: Indicates both the source and destination IP addresses
Member	Lists the member ports of the static trunk group.

Example

The following example displays information about static trunk groups on the switch:

```
awplus# show static-channel-group
```

STATIC-CHANNEL-GROUP

Syntax

```
static-channel-group id_number
```

Parameter

id_number
: Specifies the ID number of a static trunk group. The range is 1 to 32.

Mode

Port Interface mode

Description

Use this command to create a new static trunk group or to add ports to an existing static channel group. You can create up to 32 trunk groups on the switch, including dynamic LACP and static trunk groups.

To create a new static trunk group or add ports to an existing static trunk group, the member ports must belong to the same VLAN and have the same switchport mode: either access or trunk.

When you specify a static trunk group in the command line, add the prefix “sa” to the ID number. For example, A static trunk group with the ID number 3 is “sa3.”

To remove the port from the static trunk group, use the NO STATIC-CHANNEL-GROUP command.

Note
If you delete all the member ports from the LACP trunk group, the LACP trunk group is deleted automatically.

Confirmation Command

“SHOW ETHERCHANNEL” on page 288

Examples

This example creates a new static trunk group consisting of ports 1.0.11 through 1.0.16. The ID number of the LACP trunk group is 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.16
awplus(config-if)# static-channel-group 2
```

This example adds port 1.0.15 to an existing LACP trunk group that has the ID number 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# static-channel-group 2
```

This example removes port 1.0.15 from the static trunk group:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15
awplus(config-if)# no static-channel-group
```

Chapter 13
VLAN Commands

The VLAN commands are summarized in Table 54.

Table 54. Port-based and Tagged VLAN Commands

Command	Mode	Description
“INTERFACE VLAN” on page 307	Global Configuration	Enters the VLAN Interface mode from the Global Configuration mode.
“NO SWITCHPORT ACCESS VLAN” on page 308	Port Interface	Assigns untagged ports to the default VLAN 1.
“NO SWITCHPORT TRUNK” on page 309	Port Interface	Removes the tagged designation from ports.
“NO SWITCHPORT TRUNK NATIVE VLAN” on page 310	Port Interface	Reestablishes the default VLAN 1 as the native VLAN.
“NO VLAN” on page 311	VLAN Configuration	Deletes VLANs from the switch.
“NO VLAN MACADDRESS (Global Configuration Mode)” on page 312	Global Configuration	Removes a MAC address from a MAC address-based VLAN.
“NO VLAN MACADDRESS (Port Interface Mode)” on page 313	Port Interface	Removes a MAC address from egress ports.
“SHOW VLAN” on page 314	User Exec	Displays all the VLANs on the switch.
“SHOW VLAN MACADDRESS” on page 316	Privileged Exec	Displays MAC address-based VLANs.
“SWITCHPORT ACCESS VLAN” on page 318	Port Interface	Assigns a VLAN to the untagged ports.
“SWITCHPORT MODE ACCESS” on page 319	Port Interface	Enters the access mode to configure untagged ports.
“SWITCHPORT MODE TRUNK” on page 320	Port Interface	Enters the trunk mode to configure tagged ports.
“SWITCHPORT TRUNK ALLOWED VLAN” on page 322	Port Interface	Adds and removes tagged ports from VLANs.
“SWITCHPORT TRUNK NATIVE VLAN” on page 324	Port Interface	Designates native VLANs for tagged ports.
“VLAN” on page 326	VLAN Configuration	Creates port-based and MAC address-based VLANs.

Table 54. Port-based and Tagged VLAN Commands (Continued)

Command	Mode	Description
“VLAN DATABASE” on page 328	Global Configuration	Enters the VLAN Configuration mode.
“VLAN MACADDRESS” on page 329	VLAN Configuration	Create new MAC address-based VLAN.
“VLAN SET MACADDRESS (Global Configuration Mode)” on page 331	Global Configuration	Adds a MAC address to a MAC address-based VLANs.
“VLAN SET MACADDRESS (Port Interface Mode)” on page 333	Port Interface	Adds a MAC address to egress ports.

INTERFACE VLAN

Syntax

```
interface vlan_ids
```

Parameter

vlan_ids
: Specifies a VLAN ID or multiple VLAN IDs. Use a comma (,) to separate VLAN IDs and a hyphen (-) to indicate a range of VLAN IDs.

Mode

Global Configuration mode

Description

Use this command to move from the Global Configuration mode to the Port Interface mode to configure VLANs.

Example

This example moves to the VLAN Interface mode to configure VLANs 10, 20, and 30:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan10,20,30
```

NO SWITCHPORT ACCESS VLAN

Syntax

```
no switchport access vlan
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to return untagged ports on the switch to the default value of VLAN 1.

This command is equivalent to the SWITCHPORT ACCESS VLAN command with a VID of 1 specified. See “SWITCHPORT ACCESS VLAN” on page 318.

Confirmation Command

“SHOW VLAN” on page 314

Example

This example returns port 1.0.5 to the default value of VLAN 1:

```
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 change the ports to untagged ports and assign the ports to the default VLAN1 if the ports are tagged ports. This command changes the ports to the access mode so that you can configure the ports as untagged ports.

This command is equivalent to the SWITCHPORT ACCESS VLAN command. See "SWITCHPORT ACCESS VLAN" on page 318.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example changes ports 1.0.23 and 1.0.24 to untagged ports and assigns the ports to the default VLAN value of 1:

```
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 1 as the native VLAN of the tagged ports. The native VLAN is the repository for untagged frames received by tagged ports.

When the default VLAN 1 is assigned to untagged ports, this command removes the default VLAN 1 assignment from untagged ports and assigns the default VLAN 1 to the native VLAN of untagged ports.

To reestablish the default VLAN 1 as the native VLAN, ports must be tagged ports.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example reestablishes the default VLAN 1 as the native VLAN for tagged 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)# no switchport trunk native vlan
```

NO VLAN

Syntax

```
no vlan vid
```

Parameter

vid

Specifies the VID of the VLAN you want to delete. You can specify multiple VIDs. Use a comma (,) to separate VIDs and a hyphen (-) to indicate a range of VIDs.

Mode

VLAN Configuration mode

Description

Use this command to delete port-based or tagged VLANs from the switch. You cannot delete the default VLAN 1. When you delete a VLAN from the switch, the switch returns the untagged ports (assigned to the deleted VLAN) to the default VLAN as untagged ports.

Confirmation Command

"SHOW VLAN" on page 314

Example

This example deletes the VLAN with a VID value of 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 5
```

NO VLAN MACADDRESS (Global Configuration Mode)

Syntax

```
no vlan vid macaddress mac-address
```

Parameters

vid
: Specifies the VID of a MAC address-based VLAN. The MAC address-based VLAN must already exist.

mac-address
: Specifies the MAC address. You can specify only one address. The MAC address must be entered in the hexadecimal format:

  xx:xx:xx:xx:xx:xx

Mode

Global Configuration mode

Description

Use this command to remove a MAC address from a MAC address-based VLAN. You can remove only one address at a time with this command.

MAC addresses cannot be deleted if they are assigned to egress ports. To remove MAC addresses from egress ports, see “NO VLAN MACADDRESS (Port Interface Mode)” on page 313.

Confirmation Command

“SHOW VLAN MACADDRESS” on page 316

Example

This example removes the MAC address 00:30:84:32:8A:5D from a MAC address-based VLAN with a VID value of 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# no vlan 4 macaddress 00:30:84:32:8a:5d
```

NO VLAN MACADDRESS (Port Interface Mode)

Syntax

```
no vlan vid macaddress mac-address
```

Parameters

vid

Specifies the VID of a MAC address-based VLAN. The MAC address-based VLAN must already exist.

mac-address

Specifies the MAC address. You can specify only one address. The MAC address must be entered in the hexadecimal format:

xx:xx:xx:xx:xx:xx

Mode

Port Interface mode

Description

Use this command to remove a MAC address from egress ports assigned to MAC address-based VLANs. You can remove only one address at a time with this command.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 316

Example

This example removes the MAC address 00:30:84:32:8A:5D from egress ports 1.0.1 through 1.0.10 in a VLAN that has a VID value of 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-1.0.10
awplus(config-if)# no vlan 4 macaddress 00:30:84:32:8a:5d
```

SHOW VLAN

Syntax

```
show vlan
```

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display all the tagged and untagged VLANs on the switch. See Figure 57 for an example.

```
VLAN ID   Name        Type     State     Member ports
                                         (u)-Untagged, (t)-Tagged
=======   ========    ======   =======   ============================
1         default     STATIC   ACTIVE    port1.0.49(u)
10        orange      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)
                                         port1.0.49(t)
20        white       STATIC   ACTIVE    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)
                                         port1.0.29(u) port1.0.30(u)
                                         port1.0.31(u) port1.0.32(u)
                                         port1.0.49(t)
30        beige       STATIC   ACTIVE    port1.0.33(u) port1.0.34(u)
                                         port1.0.35(u) port1.0.36(u)
                                         port1.0.37(u) port1.0.38(u)
                                         port1.0.39(u) port1.0.40(u)
                                         port1.0.41(u) port1.0.42(u)
                                         port1.0.43(u) port1.0.44(u)
                                         port1.0.45(u) port1.0.46(u)
                                         port1.0.47(u) port1.0.48(u)
                                         port1.0.49(t)
100       VLAN0100    STATIC   ACTIVE    port1.0.53(u) port1.0.57(u)
                                         port1.0.61(u)
```

Figure 57. SHOW VLAN Command

The fields are described in Table 55:

Table 55. SHOW VLAN Command

Parameter	Description
VLAN ID	Indicates the ID of the VLAN.
Name	Indicates the name of the VLAN.
Type	Displays the VLAN type. The switch currently supports only static VLANs.
State	Indicates the states of the VLAN. The options are: ❒ Active: The VLAN has at least one tagged or untagged port. ❒ Inactive: The VLAN does not have any ports.
Member Ports	Lists the VLAN member ports where (u) indicates that a port is untagged and (t) indicates that a port is tagged.

Example

The following example displays all the tagged and untagged VLANs on the switch:

```
awplus# show vlan
```

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. See Figure 58 for an example.

```
VLAN 10 MAC Associations:
   Total number of associated MAC addresses: 2
   ------------------------------------------------
   MAC Address            Ports
   ------------------------------------------------
   00:00:00:01:01:01      port1.0.1-port1.0.24
   00:00:00:01:01:02      port1.0.1-port1.0.24
------------------------------------------------
VLAN 20 MAC Associations:
   Total number of associated MAC addresses: 1
   ------------------------------------------------
   MAC Address            Ports
   ------------------------------------------------
   00:00:00:02:02:01      port1.0.1-port1.0.24
   00:00:00:02:02:02      port1.0.1-port1.0.24
```

Figure 58. SHOW VLAN MACADDRESS Command

The fields are described in Table 56.

Table 56. SHOW VLAN MACADDRESS Command

Parameter	Description
VLAN *VID* MAC Associations	Indicates the VID of the MAC address-based VLAN.
Total Number of Associate MAC Addresses	Indicates the total number of MAC addresses that are assigned to the VLAN.

Table 56. SHOW VLAN MACADDRESS Command

Parameter	Description
MAC Address	Indicates the MAC addresses of the VLAN.
Ports	Indicates the egress ports.

Example

This example displays the MAC addresses and the egress ports of the MAC address-based VLANs on the switch:

```
awplus# show vlan macaddress
```

SWITCHPORT ACCESS VLAN

Syntax

```
switchport access vlan vid
```

Parameter

vid

Specifies the ID number of the VLAN to which you want to assign to the untagged ports. The range is 1 to 4094. You can specify only one VID. The specified VLAN must already exist.

Mode

Port Interface mode

Description

Use this command to assign a VLAN to untagged ports. A port can be an untagged member of only one VLAN at a time. For example, if the untagged port 1.0.5 belongs to VLAN 10 and you assign VLAN 20 to port 1.0.5 using this command, the switch removes the VLAN 10 and assigns VLAN 20 to port 1.0.5.

When an untagged port receives frames without VLAN tags, the frames are considered to belong to the VLAN that the untagged port belongs to, unless the host connected to the port matches a MAC address based-VLAN.

To assign a VLAN to untagged ports, the ports must be in the access mode.

Confirmation Command

“SHOW VLAN” on page 314

Example

This example adds ports 1.0.5 and 1.0.7 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
```

SWITCHPORT MODE ACCESS

Syntax

```
switchport mode access [ingress-filter enable|disable]
```

Parameters

`enable`
: Activates ingress filtering for tagged frames so that the ports accept only tagged frames that match the port-based VLAN ID and discards tagged frames that do not match. By default, ingress filtering is enabled.

`disable`
: Disables ingress filtering so that the ports accept all tagged frames.

Mode

Port Interface mode

Description

Use this command to change the ports to the access mode to configure as untagged ports. By default, all ports on the switch are in the access mode and belong to the default VLAN 1. Use the SWITCHPORT ACESS VLAN command to change the VLAN that the ports belong to. See "SWITCHPORT ACCESS VLAN" on page 318.

When the switch ports are labeled as tagged ports, this command changes the ports to untagged ports and assigns the ports to the default value of VLAN 1.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example changes the mode of ports 1.0.17 through 1.0.24 to the access mode:

```
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 frames that have one of its tagged VIDs and discards tagged frames that do not match. By default, ingress filtering is enabled.

`disable`
: Disabled ingress filtering so the tagged port accepts all tagged frames.

Mode

Port Interface mode

Description

Use this command to change the ports to the trunk mode to configure as tagged ports. After changing the ports to the trunk mode, use the SWITCHPORT TRUNK ALLOWED VLAN command to assign VLANs as tagged VLANS to the ports. See “SWITCHPORT TRUNK ALLOWED VLAN” on page 322.

The ingress filtering feature allows you to control whether the tagged port accepts or rejects tagged frames containing VIDs that do not match the defined tagged VIDs assigned to the port. When ingress filtering is enabled, the port accepts only frames containing VIDs that match the defined tagged VIDs to the port. When ingress filtering is disabled, the port accepts all tagged frames.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Examples

This example changes ports 1.0.4 through 1.0.6 to the trunk mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.4-port1.0.6
awplus(config-if)# switchport mode trunk
```

This example changes port 1.0.18 to the trunk mode 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

`switchport trunk allowed vlan all|none`

`switchport trunk allowed vlan add` *`vids`*

`switchport trunk allowed vlan except` *`vids`*

`switchport trunk allowed vlan remove` *`vids`*

Parameters

`all`
: Assigns all existing VLANs on the switch to the tagged ports. The ports accept any tagged frames with the VID of an existing VLAN.

`none`
: Specifies that the tagged ports do not accept any tagged frames.

add *vids*
: Adds the specified VLANs to the tagged ports. The tagged ports start accepting tagged frames with the specified VLANs. You can specify multiple VIDs. Use a comma (,) to separate VIDs and a hyphen (-) to indicate a range of VIDs.

except *vids*
: Assigns all existing VLANs on the switch, except the specified VLANs, to the tagged ports. You can specify multiple VIDs. Use a comma (,) to separate VIDs and a hyphen (-) to indicate a range of VIDs.

remove *vids*
: Removes the specified VLANs from the list of VLANs assigned to the tagged port. The tagged ports stop accepting frames with the specified VLANs. You can specify multiple VIDs at a time. Use a comma (,) to separate VIDs and a hyphen (-) to indicate a range of VIDs.

Mode

Port Interface mode

Description

Use this command to assign VLANs to tagged ports so that the tagged ports send and receive only the frames that have the IDs of the specified VLANs. You can assign multiple VLANs to tagged ports. The range of VIDs is 1 to 4094.

Note
To assign VLANs to tagged ports, the ports must be in the trunk mode. Use the SWITCHPORT MODE TRUNK command to place a port in trunk mode. See "SWITCHPORT MODE TRUNK" on page 320.

Confirmation Command

"SHOW VLAN" on page 314

Examples

This example assigns ports 1.0.18 through 1.0.20 to tagged ports and assigns all existing VLANs on the switch to the ports so that the ports accept tagged frames with the VID of an existing VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18-port1.0.20
awplus(config)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan all
```

This example assigns port 1.0.5 to a tagged port and adds VLANs 20 and 30 to the port so that the port accepts tagged frames that contain the VID 20 and 30:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 20,30
```

This example removes VLANs 5 through 8 from the list of VLANs assigned to port 1.0.10. Port 1.0.10 stops accepting frames that contain VIDs 5 through 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.10
awplus(config-if)# switchport trunk allowed vlan remove 5-8
```

This example specifies that port 1.0.19 and 1.0.22 do not accept any tagged frames:

```
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. The range is 1 to 4094. You can specify only one VID.

none
: Specifies that the tagged ports do not accept untagged frames.

Mode

Port Interface mode

Description

Use this command to designate the native VLAN for tagged ports. The native VLAN stores untagged frames received by tagged ports. A tagged port can have only one native VLAN and the VLAN must already exist on the switch. By default, the native VLAN is the set to the default VLAN 1.

Note
To assign a VLAN as the native VLAN, the ports must be in the trunk mode. Use the SWITCHPORT MODE TRUNK command to place a port in trunk mode. See “SWITCHPORT MODE TRUNK” on page 320.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Examples

This example designates VLAN 17 as the native VLAN for tagged port 1.0.15:

```
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 specifies that tagged ports 1.0.18 and 1.0.20 do not accept untagged frames:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18,port1.0.20
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk native vlan none
```

VLAN

Syntax

`vlan` *`vids`* `[name` *`vlanname`*`] [type madaddress]`

Parameters

`vids`

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 multiple VIDs at a time. Use a comma (,) to separate VIDs and a hyphen (-) to indicate the range of VIDs.

`vlanname`

Specifies a name for a new VLAN. A name can be from 1 to 32 alphanumeric characters. Spaces and special characters except hyphens (-) and underscores (_) are not allowed. The first character must be a letter. A name cannot be the same as the name of an existing VLAN on the switch. When comparing VLAN names, the switch ignores their cases. For example, the switch considers that “sales” and “Sales” are the same names. You cannot include this parameter when specifying multiple VIDs.

`type madaddress`

Creates a MAC address-based VLAN. When these keywords are not specified, a port-based VLAN is created. You cannot include these keywords when specifying multiple VIDs.

Mode

VLAN Configuration mode

Description

Use this command to create port-based and MAC address-based VLANs. You can create multiple port-based VLANs at one time; however, you cannot name multiple VLANs. If you want to name a VLAN, create one VLAN at a time. To create a MAC address-based VLAN, you must create one MAC address-based VLAN at a time. A MAC address-based VLAN can be assigned to both tagged and untagged ports.

Confirmation Command

“SHOW VLAN” on page 314 and “SHOW VLAN MACADDRESS” on page 316

Examples

This example creates new port-based VLANs with VIDs of 3, 4, 5, 6, 10, and 30:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 3-6,10,30
```

This example creates a new port-based VLAN with a VID of 100 and the name "Engineering":

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100 name Engineering
```

This example creates a new MAC address-based VLAN with a VID of 50 and the name "MAC":

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 50 name MAC type macaddress
```

VLAN DATABASE

Syntax

```
vlan database
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enter the VLAN Configuration mode to configure VLANs.

Example

This example enters the VLAN Configuration mode from the Global Configuration mode:

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

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 must be unique 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 that spans three switches, you 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 are easier to identify if their names reflect the functions of their subnetworks or work groups (for example, Sales or Accounting). A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). A name must be unique on the switch for a VLAN that is only on one switch. A VLAN that spans multiple switches must have the same name on each switch.

Mode

VLAN Configuration mode

Description

Use this command to create a MAC address-based VLAN. You can create only one VLAN at a time.

After creating a VLAN, use "SWITCHPORT ACCESS VLAN" on page 318 to add MAC addresses to it and "VLAN SET MACADDRESS (Port Interface Mode)" on page 333 to assign the address to egress ports.

Confirmation Command

"VLAN MACADDRESS" on page 329

Example

This example creates a MAC address-based VLAN that has the name “Sales” and a VID value of 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 mac-address
```

Parameters

vid

Specifies the VID of a MAC address-based VLAN. The MAC address-based VLAN must already exist.

mac-address

Specifies the MAC address. The MAC address must be entered in the hexadecimal format:

xx:xx:xx:xx:xx:xx

Mode

Global Configuration mode

Description

Use this command to add a MAC address to a MAC address-based VLAN. You can add only one address at a time. To create a MAC address-based VLAN, see "VLAN MACADDRESS" on page 329.

To forward frames from the hosts with the specified MAC addresses, you must associate the MAC address to egress ports using the VLAN SET ADDRESS (Port Interface Mode) command. See "VLAN SET MACADDRESS (Global Configuration Mode)" on page 331.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 316

Examples

This example adds the MAC address, 00:30:84:32:8A:5D, to a MAC address-based VLAN with a VID value of 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan set 4 macaddress 00:30:84:32:8a:5d
```

This example adds another MAC address, 00:30:84:32:76:1A, to a MAC address-based VLAN with a VID value of 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan set 4 macaddress 00:30:84:32:76:1a
```

VLAN SET MACADDRESS (Port Interface Mode)

Syntax

```
vlan set vid macaddress mac-address
```

Parameters

vid

Specifies the VID of a MAC address-based VLAN. The MAC address-based VLAN must already exist.

mac-address

Specifies the MAC address to assign to egress ports. The MAC address must be entered in the hexadecimal format:

xx:xx:xx:xx:xx:xx

Mode

Port Interface mode

Description

Use this command to assign MAC addresses to egress ports for MAC address-based VLANs. You can add only one address at a time. The specified MAC address must be already added to the MAC address-base VLAN with the VLAN SET MACADDRESS (Global Configuration Mode) command. See "VLAN SET MACADDRESS (Global Configuration Mode)" on page 331.

Confirmation Command

"SHOW VLAN MACADDRESS" on page 316

Example

This example assigns the MAC address 00:30:84:32:8A:5D to egress ports 1.0.1 through 1.0.10 in a VLAN whose VID value is 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-1.0.10
awplus(config-if)# vlan set 4 macaddress 00:30:84:32:8a:5d
```

Chapter 14
STP Commands

The STP commands are summarized in Table 57.

Table 57. Spanning Tree Protocol Commands

Command	Mode	Description
“CLEAR SPANNING-TREE DETECTED PROTOCOLS” on page 338	Privileged Exec	Moves the ports to the original mode from the STP-compatible mode.
“INSTANCE PRIORITY” on page 339	MST Configuration	Sets the bridge priority for an MST instance.
“INSTANCE VLAN” on page 340	MST Configuration	Create an MST instance and associate VLANs with it.
“REGION” on page 342	MST Configuration	Assigns the name of an MST region to the switch.
“REVISION” on page 343	MST Configuration	Assigns an MST revision number to the switch.
“SHOW SPANNING-TREE” on page 344	User Exec and Privileged Exec	Displays the STP, RSTP, or MSTP settings.
“SHOW SPANNING-TREE MST” on page 352	Privileged Exec	Displays the information about CIST and MST instances to VLAN mappings.
“SHOW SPANNING-TREE MST CONFIG” on page 355	Privileged Exec	Displays the MSTP Configuration information on the switch.
“SHOW SPANNING-TREE MST INSTANCE” on page 357	Privileged Exec	Displays detailed information for a particular instance.
“SPANNING-TREE ENABLE” on page 360	Global Configuration	Enables STP, RSTP, or MSTP on the switch.
“SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE” on page 362	Global Configuration	Enables the timer for the BPDU guard feature.
“SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL” on page 363	Global Configuration	Specifies the duration of the BPDU guard timer.

Table 57. Spanning Tree Protocol Commands (Continued)

Command	Mode	Description
“SPANNING-TREE FORWARD-TIME” on page 364	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 HELLO-TIME” on page 365	Global Configuration	Sets the hello time, which defines how frequently the switch sends BPDUs.
“SPANNING-TREE LINK-TYPE” on page 366	Port Interface	Specifies the link type to a port, point-to-point or shared.
“SPANNING-TREE LOOP-GUARD” on page 367	Port Interface	Enables the BPDU loop-guard feature on the ports.
“SPANNING-TREE MAX-AGE” on page 368	Global Configuration	Sets the maximum age value, which defines how long the switch saves configuration BPDU information before they are deleted.
“SPANNING-TREE MAX-HOPS” on page 369	Global Configuration	Sets the maximum number of hops.
“SPANNING-TREE MODE” on page 370	Global Configuration	Designates STP, RSTP, or MSTP as the active spanning tree protocol on the switch.
“SPANNING-TREE MST CONFIGURATION” on page 371	Global Configuration	Enters the MST Configuration mode.
“SPANNING-TREE MST INSTANCE” on page 372	Port Interface	Associates an MST instance with ports.
“SPANNING-TREE MST INSTANCE PATH-COST” on page 374	Port Interface	Specifies the cost of a port to the root bridge.
“SPANNING-TREE MST INSTANCE PRIORITY” on page 375	Port Interface	Assigns a port priority to a port for the specified MST instance.
“SPANNING-TREE PATH-COST” on page 376	Port Interface	Specifies the cost of a port to the root bridge.
“SPANNING-TREE PORTFAST” on page 378	Port Interface	Designates the ports as edge ports.
“SPANNING-TREE PORTFAST BPDU-GUARD (SWITCH)” on page 379	Global Configuration	Enables the Root Guard feature on the switch.
“SPANNING-TREE PORTFAST BPDU-GUARD (PORT)” on page 381	Port Interface	Enables the Root Guard feature on a port.

Table 57. Spanning Tree Protocol Commands (Continued)

Command	Mode	Description
"SPANNING-TREE PRIORITY (Bridge Priority)" on page 383	Global Configuration	Assigns the switch a bridge priority number.
"SPANNING-TREE PRIORITY (Port Priority)" on page 384	Port Interface	Assigns a priority value to a port.

CLEAR SPANNING-TREE DETECTED PROTOCOLS

Syntax

```
clear spanning-tree detected protocols [interface port_ids]
```

Parameter

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

Privileged Exec mode

Description

Use this command to move the specified ports to the original RSTP or MSTP mode from the STP mode. When you do not specify a port or multiple ports, this command moves all the ports on the switch to the original mode.

Note
This command is applicable only when RSTP or MSTP is enabled.

In the RSTP or MSTP mode, the switch automatically moves to the STP mode when receiving STP BPDUs. The switch does not return to the original RSTP or MSTP mode even when the switch no longer receives STP BPDUs. However, in the STP mode, when the switch receives RSTP or MSTP BPDUs, the switch automatically returns to the original STP mode.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example moves all the ports on the switch to the original mode from the STP mode:

```
awplus> enable
awplus# clear spanning-tree detected protocols
```

INSTANCE PRIORITY

Syntax

```
instance mst-instance priority priority
```

Parameters

mst-instance
: Specifies the ID number of an MST instance. The range is from 1 to 15.

priority
: Specifies a bridge priority for the specified MST instance. The range is 0 to 61,440, in increments of 4,096. Specify 0, 4096, 8192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, or 61,440 (without commas). The default value is 32,768.

Mode

MST Configuration mode

Description

Use this command to set a bridge priority for the specified MST instance on the switch. A lower bridge priority value gives the switch a higher priority.

Note
This command is applicable only when MSTP is enabled.

To restore the default value of 32,768, use the NO INSTANCE PRIORITY command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example assigns a bridge priority of 4,096 to MST instance 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 1 priority 4096
```

INSTANCE VLAN

Syntax

instance *mst-instance* vlan *vlan_ids*

Parameters

mst-instance
Specifies the ID number of an MST instance. The range is from 1 to 15.

vlan_ids
Specifies a VLAN ID or multiple VLAN IDs. Use a comma (,) to separate VLAN IDs and a hyphen (-) to indicate a range of VLAN IDs.

Mode

MST Configuration mode

Description

Use this command to create an MST instance and associate it with one or more VLANs. When specifying an existing MST instance, you can change VLANs that you want to associate with the MST instance.

Note
This command is applicable only when MSTP is enabled.

The switch supports up to 15 MST instances. An instance can contain any number of VLANs, but a VLAN can belong to only one MST instance at a time.

After creating an MST instance and associating it with a VLAN, use the SPANNING-TREE MST INSTANCE command to associate ports with each instance. See “SPANNING-TREE MST INSTANCE” on page 372.

By default, all the VLANs on the switch are associated with CIST (with an instance value of 0). This command removes the specified VLANs from CIST and assigns them to the specified MST instance.

To remove a VLAN association from the MST instance, use the NO INSTANCE VLAN command with the vlan_ids parameter. After the VLAN is removed from the MST instance, the VLAN belongs to CIST (with an instance value of 0) again. When you do not specify VLAN IDs, this command deletes the specified MST instance from the switch.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example assigns an MSTI ID of 1 to VLAN 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# instance 1 vlan 10,20,30
```

REGION

Syntax

```
region region_name
```

Parameter

region_name
: Specifies the name of an MST region. The name can be up to 32 alphanumeric characters. Underscores (_) and hyphens (-) are permitted. By default, no name is assigned.

Mode

MST Configuration mode

Description

Use this command to name the MST region. When you want a group of switches to belong to the same region, assign the same MST region name and the same revision number to these switches.

Note
This command is applicable only when MSTP is enabled.

To delete the MST region name, use the NO REGION command.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example names the MSTP region named “Test”:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus (config-mst)# region Test
```

REVISION

Syntax

```
revision revision_number
```

Parameter

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 on the switch. Use the revision number to track the number of times an MST configuration has been updated on the network.

Note
This command is available only when MSTP is enabled.

When you want a group of switches to belong to the same region, you must assign the same MST region name and the same revision number to these switches.

To restore the default revision number of 0, use the NO REVISION command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example specifies the MST revision number as 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus (config-mst)# revision 4
```

SHOW SPANNING-TREE

Syntax

`show spanning-tree [interface` *`port_ids`*`]`

Parameter

`port_ids`

Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Modes

Privileged Exec mode

Description

Use this command to display the STP settings on the switch. See Figure 59 for an example of the display.

```
% Default: Bridge up - Spanning Tree Enabled
% Default: Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 8000001477000000
% Default: Bridge Id 8000001477000000
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%  port1.0.1: Port Id 8101 - Role Designated - State Forwarding
%  port1.0.1: Designated Path Cost 0
%  port1.0.1: Configured Path Cost 2000 - Add type Explicit ref count 1
%  port1.0.1: Designated Port Id 8101 - Priority 128 -
%  port1.0.1: Root 8000001477000000
%  port1.0.1: Designated Bridge 8000001477000000
%  port1.0.1: Message Age 0 - Max Age 20
%  port1.0.1: Hello Time 2 - Forward Delay 15
%  port1.0.1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 2 - topo
change timer 0
%  port1.0.1: Version Spanning Tree Protocol
%  port1.0.1: No portfast configured - Current portfast off
%  port1.0.1: portfast bpdu-guard default - Current portfast bpdu-guard
off
%  port1.0.1: no loopguard configured
%  port1.0.1: Configured Link Type auto
. . .
```

Figure 59. SHOW SPANNING-TREE Command

Table 58 describes the fields for displaying when STP or RSTP is enabled.

Table 58. SHOW SPANNING-TREE Command for STP & RSTP

Field	Description
Spanning Tree	Displays the status of the Spanning Tree Protocol on the switch. The options are: ❒ Enabled ❒ Disabled
Bridge Priority	Displays the value of the bridge priority specified for the switch.
Forward Delay	Displays the value of forward delay specified for the switch.
Hello Time	Displays the hello time specified for the switch.
Max Age	Displays the maximum aging time specified for the switch.
Root Id	Displays the bridge ID of the root bridge.
Bridge Id	Displays the bridge ID of the switch.
portfast bpdu-guard	Displays the status of the BPDU guard feature on the switch. The options are: ❒ Enabled ❒ Disabled
portfast errdisable timeout	Displays whether the switch reactivates the disabled edge ports after the specified time period.
portfast errdisable timeout interval	Displays the number of seconds that must elapse before the switch automatically reactivates the disabled edge ports.
For port	
portX.X.X	Displays the port ID on the switch.
Port Id	Displays the port ID for Spanning Tree Protocol.

Table 58. SHOW SPANNING-TREE Command for STP & RSTP

Field	Description
Role	Displays the port role. The options are: ❒ Disabled ❒ Alternate ❒ Backup ❒ Root ❒ Designated ❒ Loop Guard
State	Displays the state of the port. The options are: ❒ Disabled ❒ Discarding ❒ Learning ❒ Forwarding
Designated Path Cost	Displays the path cost to the root bridge that is notified by the designated port.
Configured Path Cost	Displays the path cost assigned to the port.
Designated Port Id	Displays the designated port ID for spanning tree protocol.
Priority	Displays the port priority of the port.
Designated Bridge	Displays the bridge ID of the designated bridge.
Message Age	Displays the time that it takes to transmit a message from the root bridge, The time depends upon the distance to the root bridge.
Max Age	Displays the maximum aging time for the root bridge.
Hello Time	Displays the hello time of the root bridge.
Forward Delay	Displays the forward delay time of the root bridge.
Forward Timer	Displays the value of the forward timer.
Msg Age Timer	Displays the time that a message from the root bridge expires.
Hello Timer	Displays the value of the hello timer.
topo change timer	Displays the time between a topology change occurred and the time it is recognized.

Table 58. SHOW SPANNING-TREE Command for STP & RSTP

Field	Description
Version	Displays the version of the Spanning Tree Protocol. The options are: ❒ Spanning Tree Protocol ❒ Rapid Spanning Tree Protocol ❒ Multiple Spanning Tree Protocol
portfast configured	Displays whether the port is configured as an edge port.
Current portfast	Displays whether the port is active or not active as an edge port. The options are: ❒ On ❒ Off
portfast bpdu-guard	Displays the setting of the BPDU guard feature on the port. The options are: ❒ Enabled ❒ Disabled ❒ Default
Current portfast bpdu-guard	Displays whether the BPDU guard feature is on or off on the port.
loop guard	Displays whether the loop guard feature is on or off on the port.
Link Type	Displays the link type of the port. The options are: ❒ auto ❒ point-to-point ❒ shared

Table 59.describes the fields for displaying when MSTP is enabled.

Table 59. SHOW SPANNING-TREE Command for MSTP

Field	Description
Spanning Tree	Displays the status of the Spanning Tree Protocol on the switch. The options are: ❒ Enabled ❒ Disabled

Table 59. SHOW SPANNING-TREE Command for MSTP (Continued)

Field	Description
CIST Root Path Cost	Displays the path cost to the region that the CIST root bridge belongs to (External Root Path Cost).
CIST Root Port	Displays the ID of the CIST root port.
CIST Bridge Priority	Displays the CIST bridge priority on the switch.
Forward Delay	Displays the value of forward delay specified for the switch.
Hello Time	Displays the hello time specified for the switch.
Max Age	Displays the maximum aging time specified for the switch.
Max-hops	Displays the maximum number of hops on the switch.
CIST Root Id	Displays the bridge ID of the CIST root bridge.
CIST Reg Root Id	Displays the bridge ID of the regional root bridge.
Bridge Id	Displays the bridge ID of the switch.
last topology change	Displays the most recent date the topology changed.
portfast bpdu-guard	Displays whether the BPDU guard feature is enabled or disabled.
portfast errdisable timeout	Displays whether the switch automatically reactivates disabled ports after the specified time period.
portfast errdisable timeout interval	Displays the time interval that ports remain disabled before the switch automatically enables the disabled ports
For port	
portX.X.X	Displays the port ID on the switch.
Port Id	Displays the port ID for Spanning Tree Protocol.

Table 59. SHOW SPANNING-TREE Command for MSTP (Continued)

Field	Description
Role	Displays the port role. The options are: ❒ Disabled ❒ Alternate ❒ Backup ❒ Root ❒ Designated ❒ LoopGuard
State	Displays the state of the port. The options are: ❒ Disabled ❒ Discarding ❒ Learning ❒ Forwarding
Designated External Path Cost	Displays the path cost, notified by the designated port, that belongs to another region. It is the path cost of the region that the CIST root bridge belongs to.
Internal Path Cost	Displays the path cost, notified by the designated port, that belongs to the same region. It is the path cost of the CIST regional root bridge.
Configurated Path Cost	Displays the path cost configured on the port.
Designated Port Id	Displays the designated port ID for the Spanning Tree Protocol.
CIST Priority	Displays the port priority of the port.
CIST Root	Displays the bridge ID of the CIST root bridge.
Designated Bridge	Displays the bridge ID of the designated bridge.
Message Age	Displays the time that it takes to transmit a message from the root bridge, The time depends upon the distance to the root bridge.
Max Age	Displays the maximum aging time for the root bridge.
CIST Hello Time	Displays the hello time of the root bridge.

Table 59. SHOW SPANNING-TREE Command for MSTP (Continued)

Field	Description
Forward Delay	Displays the forward delay time of the root bridge.
CIST Forward Timer	Displays the value of the forward timer.
Msg Age Timer	Displays the time that a message from the root bridge expires.
Hello Timer	Displays the value of the hello timer.
topo change timer	Displays the time between a topology change occurred and the time it is recognized.
Version	Displays the version of Spanning Tree Protocol. The options are: ❒ Spanning Tree Protocol ❒ Rapid Spanning Tree Protocol ❒ Multiple Spanning Tree Protocol
portfast configured	Displays whether the port is configured as an edge port.
Current portfast	Displays whether the port is active or not active as an edge port. The options are: ❒ On ❒ Off
portfast bpdu-guard	Displays the setting of the BPDU guard feature on the port. The options are: ❒ Enabled ❒ Disabled ❒ Default
Current portfast bpdu-guard	Displays whether the BPDU guard feature is on or off on the port.
loop guard	Displays whether the loop guard feature is on or off on the port.
Link Type	Displays the link type of the port. The options are: ❒ auto ❒ point-to-point ❒ shared

Examples

This command displays the STP, RSTP, or MSTP settings for all of the ports:

```
awplus# show spanning-tree
```

This command displays the STP, RSTP, or MSTP settings for ports 1.0.1 and 1.0.2:

```
awplus# show spanning-tree interface port1.0.1,port1.0.2
```

SHOW SPANNING-TREE MST

Syntax

```
show spanning-tree mst
```

Parameters

None

Mode

Privileged Executive Mode

Description

Use this command to display information about CIST (instance: 0) and associations between MST instances and VLANs.

Note
This command is available only when MSTP is enabled.

See Figure 60 for an example of the command output.

```
% 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 0
%  Default: CIST Root Id 800000147000000
%  Default: CIST Reg Root ID 8000001477000000
%  Default: CIST Bridge Id 8000001477000000
%  Default: CIST 5 topology change(s) - last topology change Sat Sep 29
11:04:29:2021
%
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%
% Instance       VLAN
%  0       :     1
%  1       :     2
```

Figure 60. SHOW SPANNING-TREE MST Command

The fields are described in Table 60.

Table 60. SHOW SPANNING-TREE MST Command

Field	Description
Spanning Tree	Displays whether the Spanning Tree Protocol is enabled or disabled.
CIST Root Path Cost	Displays the path cost to the region that the CIST root bridge belongs to (External Root Path Cost).
CIST Root Port	Displays the ID of the CIST root port.
CIST Bridge Priority	Displays the CIST bridge priority on the switch.
Forward Delay	Displays the forward delay time of the switch.
Hello Time	Displays the hello time of the switch.
Max Age	Displays the maximum aging time for the switch.
Max-hops	Displays the maximum number of hops on the switch.
CIST Root Id	Displays the bridge ID of the CIST root bridge.
CIST Reg Root Id	Displays the bridge ID of the regional root bridge.
CIST Bridge Id	Displays the bridge ID of the switch.
CIST X topology change(s)	Displays the number of topology changes.
last topology change	Displays the most recent date the topology changed.
portfast bpdu-guard	Displays whether the BPDU guard feature is enabled or disabled.
portfast errdisable timeout	Displays whether the switch automatically reactivates disabled ports after the specified time period.
portfast errdisable timeout interval	Displays the time interval that ports remain disabled before the switch automatically enables the disabled ports
Instance	Displays the MST instance ID.
VLAN	Displays the VLAN IDs that belong to the MST instance.

Example

This example displays information about CIST (instance: 0) and MST instance to VLAN mappings:

```
awplus> enable
awplus# show spanning-tree mst
```

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 on the switch. Within this command display, switches with the same settings belong to the same MST region.

> **Note**
> This command is applicable only when MSTP is enabled.

See Figure 61 for an example of this command.

```
%
% MSTP Configuration Information for bridge 0:
% --------------------------------------------------------
%  Format Id          : 0
%  Name               : Test
%  Revision Level     : 1
%  Digest             : 0x9357EBB7A8D74DD5FEF4F2BAB50531AA
%  --------------------------------------------------------
```

Figure 61. SHOW SPANNING-TREE MST CONFIG Command

The fields are described in Table 61.

Table 61. SHOW SPANNING-TREE MST CONFIG Command

Field	Description
Format Id	Displays the value of the format selector. It shows always "0," meaning MSTP.
Name	Displays the name of MST region.

Table 61. SHOW SPANNING-TREE MST CONFIG Command (Continued)

Field	Description
Revision	Displays the revision number for the MST region.
Digest	Displays the message digest (HMAC-MD5) MST of the mapping table for MST instances and VLANs.

Example

This example displays the MSTP configuration on the switch:

```
awplus> enable
awplus# show spanning-tree mst config
```

SHOW SPANNING-TREE MST INSTANCE

Syntax

```
show spanning-tree mst instance mst-instance [interface
port_ids]
```

Parameters

mst-instance
Specifies the ID number of an existing MST instance. The range is from 1 to 15.

port_ids
Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

Privileged Executive Mode

Description

Use this command to display information about the ports of the specified MST instance. When the port parameter is not specified, the command displays information about all the ports that belong to the MST instance. See Figure 62 for an example of the command output.

Note
This command is available only when MSTP is enabled.

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8001001477000000
% 1: MSTI Bridge Id 8001001477000000
% 1: 9 topology changes - last topology change Sat Sep 29 11:05:42 2021

%  port1.0.1: Ifindex 257 - Port Id 8101 - Role Designated - State Forwarding
%  port1.0.1: Designated Internal Path Cost 0 - Designated Port Id 8101
%  port1.0.1: Configured Internal Path Cost 2000
%  port1.0.1: CST Priority 128 - MSTI Priority 128
%  port1.0.1:
%  port1.0.1: Designated Root 8001001477000000
%  port1.0.1: Designated Bridge 8001001477000000
%  port1.0.1: Message Age 0 - Max Age 20
%  port1.0.1: Hello Time 2 - Forward Delay 15
```

Figure 62. SHOW SPANNING-TREE MST INSTANCE Command

The fields are described in Table 62.

Table 62. SHOW SPANNING-TREE MST INSTANCE Command

Field	Description
MSTI Root Path Cost	Displays the MSTI path cost notified by the designated port. It is the path cost to the root bridge of the MSTI.
MSTI Root Port	Displays the ID of the MSTI root port.
MSTI Bridge Priority	Displays the CIST bridge priority on the switch.
MSTI Root Id	Displays the bridge ID of the MSTI root bridge.
MSTI Bridge Id	Displays the bridge ID of the switch.
X topology changes	Displays the number of topology changes.
last topology change	Displays the most recent date the topology changed.
For port	
portX.X.X	Displays the port ID on the switch.
Ifindex	Displays the index number of the port.
Port Id	Displays the port ID for Spanning Tree Protocol.
Role	Displays the port role. The options are: ❒ Disabled ❒ Alternate ❒ Backup ❒ Root ❒ Designated ❒ LoopGuard
State	Displays the state of the port. The options are: ❒ Disabled ❒ Discarding ❒ Learning ❒ Forwarding
Designated Internal Path Cost	Displays the path cost notified by the designated port. It is the path cost to the root bridge of the MST instance.

Table 62. SHOW SPANNING-TREE MST INSTANCE Command

Field	Description
Designated Port Id	Displays the designated port ID for spanning tree protocol.
Configured Internal Path Cost	Displays the internal path cost (MSTI path cost) that is configured on the port.
Configurated CST External Path Cost	Displays the external path cost (CIST path cost) that is configured on the port.
CST Priority	Displays the CIST port priority of the port.
MSTI Priority	Displays the MSTI port priority of the port.
CIST Root	Displays the bridge ID of the CIST root bridge.
Designated Root	Displays the bridge ID of the root bridge.
Designated Bridge	Displays the bridge ID of the designated bridge.
Message Age	Displays the time that a message transmits from the root bridge, The time depends upon the distance to the root bridge.
Max Age	Displays the maximum aging time for the root bridge.
Hello Time	Displays the hello time of the root bridge.
Forward Delay	Displays the forward delay time of the root bridge.
Forward Timer	Displays the value of the forward timer.
Msg Age Timer	Displays the time that a message from the root bridge expires.
Hello Timer	Displays the value of the hello timer.

Example

This example displays detailed information about all the ports of MST instance 1:

```
awplus> enable
awplus# show spanning-tree mst instance 1
```

SPANNING-TREE ENABLE

Syntax

```
spanning-tree stp|rstp|mstp enable
```

Parameters

`stp`
: Enables STP (IEEE 802.1D).

`rstp`
: Enables RSTP (IEEE 802.1w). By default, RSTP is enabled on the switch.

`mstp`
: Enables MSTP (IEEE 802.1s).

Mode

Global Configuration mode

Description

Use this command to enable one of the Spanning Tree Protocol versions: STP, RSTP, or MSTP. When the version is specified on the switch using the SPANNING-TREE MODE command, the switch enables the specified STP version.

The Spanning Tree Protocol and Router Redundancy Protocol (RRP) Snooping cannot be enabled at the same time. Disable RRP when you enable STP, RSTP, or MSTP on the switch.

To disable STP, RSTP, or MSTP, use the NO SPANNING ENABLE command.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116 or “SHOW SPANNING-TREE” on page 344

Examples

This example enables RSTP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

This example disables RSTP on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
```

SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE

Syntax

```
spanning-tree errdisable-timeout enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the timer for the BPDU guard feature. The BPDU guard feature disables ports when they receive BPDUs. When the timer is activated, the switch automatically reactivate disabled ports after the specified time period. By default, the timer is disabled and it is set to 300 seconds.

> **Note**
> This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

To change the time interval that ports remain disabled, use the SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL command. See “SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL” on page 363.

To disable the timer for the BPDU guard feature, use the NO SPANNING-TREE PORTFAST BPDU-GUARD command.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

The following example enables 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
```

Parameter

interval

Specifies the number of seconds that ports remain disabled by the BPDU guard feature. The range is 10 to 1,000,000 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 enable the timer, refer to "SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 362.

Note
This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

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 116

Example

This example sets the time interval to 500 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout interval
500
```

SPANNING-TREE FORWARD-TIME

Syntax

```
spanning-tree forward-time forwardtime
```

Parameter

forwardtime
: Specifies the forward time in seconds. The range is 4 to 30 seconds. The default is 15 seconds.

Mode

Global Configuration mode

Description

Use this command to change the forward time value on the switch. The forward time decides how long the ports remain in the listening and learning states before they transition to the forwarding state.

The forwarding time is active only if the switch is in a role of the root bridge in the spanning tree domain. The other switches in the domain 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)

When MSTP is enabled, this command sets the value to the CIST (instance 0).

To restore the default 15 seconds, use the NO SPANNING-TREE FORWARD-TIME command.

Confirmation Command

“SHOW SPANNING-TREE” on page 344

Example

This example set the forward time on the switch to 25 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forward-time 25
```

SPANNING-TREE HELLO-TIME

Syntax

```
spanning-tree hello-time hellotime
```

Parameter

hellotime
: Specifies the hello time in seconds. The range is 1 to 10 seconds. The default is 2 seconds.

Mode

Global Configuration mode

Description

Use this command to change the hello time value on the switch. The hello time controls how frequently the switches in the spanning-tree domain send Bridge Protocol Data Units (BPDUs).

The hello time is active only if the switch is in a role of the root bridge in the spanning tree domain. The other switches in the domain use a dynamic value supplied by the root bridge.

The forward time, max-age and hello time values 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)

When MSTP is enabled, this command sets the value to the CIST (instance 0).

To restore the default 2 seconds, use the NO SPANNING-TREE HELLO-TIME command.

Confirmation Command

"SHOW SPANNING-TREE" on page 344

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 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. Specify point-to-point when a port has only one spanning-tree bridge connected.

shared
: Disables rapid transition of a port. Specify shared when a port is connected to a hub with multiple spanning-tree bridges connected.

Mode

Port Interface mode

Description

Use this command to specify the link type to a port: point-to-point or shared. By default, no value is specified.

> **Note**
> This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

To reset the link type on a port, use the NO SPANNING-TREE LINK-TYPE command.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example designates ports 1.0.11 to 1.0.20 as point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.11-port1.0.20
awplus(config-if)# spanning-tree link-type point-to-point
```

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 a port. If a loop-guard enabled port stops receiving BPDU packets, the switch automatically blocks the port to prevent a loop from occurring. The port remains in the blocking state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on a port is disabled.

Note
This command is applicable only when RSTP or MSTP is enabled.

To disable the look guard feature on a port, use the NO SPANNING-TREE LOOP-GUARD command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Example

This example activates the BPDU loop-guard feature on ports 1.0.1 to 1.0.48:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.48
awplus(config-if)# spanning-tree loop-guard
```

SPANNING-TREE MAX-AGE

Syntax

```
spanning-tree max-age maxage
```

Parameter

maxage
: Specifies the maximum aging value. 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 value. The maximum age determines how long the switch saves configuration BPDU information before it is deleted.

The max-age is active only if the switch is in a role of the root bridge of the spanning tree domain. The other switches in the domain 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)

When MSTP is enabled, this command sets the value to the CIST (instance 0).

To restore the default value of 20 seconds, use the NO SPANNING-TREE MAX-AGE command.

Confirmation Command

“SHOW SPANNING-TREE” on page 344

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 MAX-HOPS

Syntax

```
spanning-tree max-hops maxage
```

Parameter

maxage
: Specifies the maximum number of hops. The range is 1 to 40 hops. The default is 20 hops.

Mode

Global Configuration mode

Description

Use this command to set the maximum number of hops that BPDUs can be forwarded to.

> **Note**
> This command is applicable only when MSTP is enabled.

To restore the default 20 hops, use the NO SPANNING-TREE MAX-HOPS command.

Confirmation Command

"SHOW SPANNING-TREE" on page 344

Example

This example sets the maximum number of hops to 40 hops:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree max-hops 40
```

SPANNING-TREE MODE

Syntax

```
spanning-tree mode stp|rstp|mstp
```

Parameters

`stp`
Specifies STP (IEEE 802.1D).

`rstp`
Specifies RSTP (IEEE 802.1w). This is the default setting.

`mstp`
Specifies MSTP (IEEE 802.1s).

Mode

Global Configuration mode

Description

Use this command to designate STP, RSTP or MSTP as the active Spanning Tree Protocol. When you change the active Spanning Tree Protocol, the settings for the previously active Spanning Tree Protocol are restored to their default values.

When the active Spanning Tree Protocol is specified on the switch, the switch enables the specified STP version.

When the Spanning Tree Protocol and Router Redundancy Protocol (RRP) Snooping cannot be enabled at the same time. Disable RRP when you enable STP, RSTP, or MSTP on the switch.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

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 MST CONFIGURATION

Syntax

```
spanning-tree mst configuration
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enter the MST mode to configure MSTP. Set the spanning-tree mode to MSTP using "SPANNING-TREE MODE" on page 370 before using this command.

Example

This example enters the MST mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mstp mode
awplus(config)# spanning-tree configuration mstp
```

SPANNING-TREE MST INSTANCE

Syntax

```
spanning-tree mst instance mst-instance
```

Parameter

mst-instance
Specifies the ID of an existing MST instance. The range is 1 to 15.

Mode

Port Interface mode

Description

Use this command to reassociate a Multiple Spanning Tree (MST) instance with a port after removing this association with the NO SPANNING-TREE MST INSTANCE command. By default, a port is associated with the MST instance of the VLAN assigned to the port. To associate an MST instance with a VLAN, see “INSTANCE VLAN” on page 340.

Note
This command is applicable only when MSTP is enabled. When MSTP is enabled, a port on the switch is always assigned to CIST (instance 0) even when the port belongs to a VLAN.

To remove an MST instance associated with a port, use the NO SPANNING-TREE MST INSTANCE command.

Confirmation Command

“SHOW SPANNING-TREE” on page 344

Examples

This example removes the association between MST instance 2 and ports 1.0.1 to 1.0.10:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-1.0.10
awplus(config-if)# no spanning-tree mst instance 2
```

This example re-associates ports 1.0.1 to 1.0.10 with MST instance 2:

```
awplus(config)# interface port1.0.1-1.0.10
awplus(config-if)# spanning-tree mst instance 2
```

SPANNING-TREE MST INSTANCE PATH-COST

Syntax

```
spanning-tree mst instance mst-instance path-cost path-cost
```

Parameters

mst-instance
Specifies the ID of an existing MST instance. The range is 1 to 15.

path-cost
Specifies the cost of a port to the root bridge of the MST instance. The range is 1 to 200,000,000. By default, the path costs are 2000 for 10Gbps ports and 1400 for 40Gbps ports.

Mode

Port Interface mode

Description

Use this command to specify the cost of a port to the root bridge of the MST instance. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. A lower path cost gives the port a higher priority.

Note
This command is applicable only when MSTP is enabled.

To restores the default path cost, use the NO SPANNING-TREE MST INSTANCE PATH-COST command.

Confirmation Command

"SHOW SPANNING-TREE" on page 344

Example

This example assigns a port cost of 500 for MST instance 2 on port 1.0.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 2 path-cost
500
```

SPANNING-TREE MST INSTANCE PRIORITY

Syntax

```
spanning-tree mst instance mst_instance priority priority
```

Parameters

mst_instance
Specifies the ID of an existing MST instance. The range is 1 to 15.

priority
Specifies a port priority for the specified MST instance. The range is 0 to 240, in increments of 16. Specify 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, or 240. The default value is 128.

Mode

Port Interface mode

Description

Use this command to assign a port priority to a port for the specified MST instance. A lower port priority value gives a port a higher priority.

Note
This command is applicable only when MSTP is enabled.

To restore the default port priority of 128, use the NO SPANNING-TREE MST INSTANCE PRIORITY command.

Confirmation Command

"SHOW SPANNING-TREE" on page 344

Example

This example assigns port 1.0.2 a port priority of 240 for MST instance 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 priority 240
```

SPANNING-TREE PATH-COST

Syntax

```
spanning-tree path-cost path-cost
```

Parameter

path-cost

Specifies the cost of a port to the root bridge. The range is 1 to 200,000,000. By default, the path costs are 2,000 for 10Gbps ports and 1400 for 40Gbps ports. When MSTP is enabled, specify the cost of a port to the CIST regional route.

Mode

Port Interface mode

Description

Use this command to specify the cost of a port to the root bridge.

Note
This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

To restore the path cost to the default value, use the NO SPANNING-TREE PATH-COST command.

Confirmation Command

“SHOW SPANNING-TREE” on page 344

Example

This example sets the path cost on port 1.0.2 to 2,500:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# spanning-tree path-cost 2500
```

This example restores the default value of the path cost on port 1.0.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# no spanning-tree path-cost
```

SPANNING-TREE PORTFAST

Syntax

```
spanning-tree portfast
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to designate edge ports on the switch. The designated edge ports transition to the forwarding state, skipping other STP stages, without waiting for spanning-tree to converge. In addition, the switch does not notify a topology change to the root bridge when detecting a change on the designated ports. Designate ports as edge ports *only* when they are not connected to switches or to LANs that have switches.

> **Note**
> This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

When the designated edge port begins receiving BPDUs, it is no longer considered an edge port by the switch; when the designated edge port stops receiving BPDUs, it is considered an edge port again. By default, all ports on the switch are not designated as edge ports.

To remove ports as edge ports, use the NO SPANNING-TREE PORTFAST command.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example configures port 1.0.17 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 (SWITCH)

Syntax

```
spanning-tree portfast bpdu-guard
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the BPDU guard feature on the switch, which disables the designated edge ports when these ports receive BPDUs. By default, the BPDU guard feature is disabled.

> **Note**
> This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

To enable the disabled edge ports manually, use the NO SHUTDOWN command. See "NO SHUTDOWN" on page 254. When the timer for the BPDU guard feature is enabled using the SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE command, the switch reactivates once disabled ports automatically. See "SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 362. The time interval that ports remain disabled is set with the SPANNING-TREE ERRDISABLE-TIMEOUT command. See "SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL" on page 363.

To enable the BPDU guard feature on each port on the switch, use the SPANNING-TREE PORTFAST BPDU-GUARD (PORT) command. The setting for the BPDU guard feature on the port *overrides* the setting for the BPDU guard feature on the switch. See "SPANNING-TREE PORTFAST BPDU-GUARD (PORT)" on page 381.

To disable the BPDU guard feature, use the NO SPANNING-TREE PORTFAST BPDU-GUARD command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example enables the BPDU guard feature on the switch so that the designated edge ports that receive BPDUs are disabled:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

This example enable a designated edge port that was disabled by the BPDU guard feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config)# no shutdown
```

SPANNING-TREE PORTFAST BPDU-GUARD (PORT)

Syntax

```
spanning-tree portfast bpdu-guard enable|disable|default
```

Parameters

`enable`
Enables the BPDU guard feature on a port.

`disable`
Disables the BPDU guard feature on a port.

`default`
Sets the setting of the BPDU guard feature on a port to default. When the setting is default, the setting of the BPDU guard feature on the switch determines the setting for all the ports on the switch. This is the default setting.

Mode

Port Interface mode

Description

Use this command to set the setting of the BPDU guard feature on a port to enable, disable, or default. When the setting of the BPDU guard feature on a port is enabled, the switch disable the port if the port is a designated edge port and receives BPDUs.

Note
This command is applicable only when RSTP or MSTP is enabled. When MSTP is enabled, this command sets the value to the CIST (instance 0).

To enable the disabled edge ports manually, use the NO SHUTDOWN command. See "NO SHUTDOWN" on page 254. When the timer for the BPDU guard feature is enabled using the SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE command, the switch reactivates once disabled ports automatically. See "SPANNING-TREE ERRDISABLE-TIMEOUT ENABLE" on page 362. The time interval that ports remain disabled is set with the SPANNING-TREE ERRDISABLE-TIMEOUT command. See "SPANNING-TREE ERRDISABLE-TIMEOUT INTERVAL" on page 363.

The setting for the BPDU guard feature on a port *overrides* the setting for the BPDU guard feature on the switch which is set with the SPANNING-

TREE PORTFAST BPDU-GUARD (SWITCH) command. See “SPANNING-TREE PORTFAST BPDU-GUARD (SWITCH)” on page 379.

To reset the BPDU guard feature setting on a port to default, use the NO SPANNING-TREE PORTFAST BPDU-GUARD (PORT) command.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Examples

This example enables the BPDU guard feature on the switch except port 1.0.12:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
awplus(config)# interface port1.0.12
awplus(config-if)# spanning-tree portfast bpdu-guard disable
```

This example resets the setting of port 1.0.12 to default so that the BPDU guard feature for port 1.0.12 depends upon the setting of the BPDU guard feature for the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
awplus(config)# interface port1.0.12
awplus(config-if)# no spanning-tree portfast bpdu-guard
```

SPANNING-TREE PRIORITY (Bridge Priority)

Syntax

```
spanning-tree priority priority
```

Parameter

priority
: Specifies a bridge priority value for the switch. The range is 0 to 61,440, in increments of 4,096. Specify 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440. The default value is 32,768.

Mode

Global Configuration mode

Description

Use this command to assign the switch a bridge priority number. A lower bridge priority value gives the switch a higher priority.The bridge priority is used to influence which switch in the spanning tree domain becomes the root bridge. The device that has the lowest bridge priority number becomes the root bridge. If two or more devices have the same bridge priority value, the device with the numerically lowest MAC address becomes the root bridge.

To restore the default value, 32,768, use the NO SPANNING-TREE PRIORITY command in the Global Configuration mode.

Confirmation Command

"SHOW SPANNING-TREE" on page 344

Example

This example sets the priority value of the switch to 8192:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree priority 8192
```

SPANNING-TREE PRIORITY (Port Priority)

Syntax

```
spanning-tree priority priority
```

Parameter

priority
: Specifies the priority value for a port. The range is 0 to 240, in increments of 16. Specify 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, or 240. The default value is 128.

Mode

Port Interface mode

Description

Use this command to set the priority value of a port. The port priority is used as a tie breaker to decide the port role when two or more ports have equal costs to the root bridge. A lower port priority value gives a port the higher priority.

When MSTP is enabled, this command sets the value to the CIST (instance 0).

To restore the default value, 128, use the NO SPANNING-TREE PRIORITY command in the Port Interface mode.

Confirmation Command

“SHOW SPANNING-TREE” on page 344

Example

This example assigns ports 1.0.16 and 1.0.17 a port priority value of 112:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.16,port1.0.17
awplus(config-if)# spanning-tree priority 112
```

Chapter 15

MAC Address Table Commands

The MAC address table commands are summarized in Table 63.

Table 63. MAC Address Table Commands

Command	Mode	Description
“CLEAR MAC ADDRESS-TABLE” on page 386	Privileged Exec	Deletes MAC address entries from the MAC address table.
“MAC ADDRESS-TABLE AGEING-TIME” on page 388	Global Configuration	Sets the aging timer, which is used by the switch to identify inactive dynamic entries of MAC addresses for deletion from the table.
“MAC ADDRESS-TABLE STATIC” on page 390	Global Configuration	Adds static entries of MAC addresses to the MAX address table on the switch.
“NO MAC ADDRESS-TABLE STATIC” on page 392	Global Configuration	Deletes static entries of MAC addresses from the MAC address table on the switch.
“SHOW MAC ADDRESS-TABLE” on page 394	Privileged Exec	Displays the MAC address table and the aging timer.

CLEAR MAC ADDRESS-TABLE

Syntax

`clear mac address-table static|dynamic [vlan` *vid* `|interface` *port_id*`s|address` *macaddress*`]`

Parameters

`static`
: Deletes static addresses.

`dynamic`
: Deletes dynamic MAC addresses.

vid
: Specifies the VLAN ID. MAC addresses that belong to the VLAN are deleted. The range is 1 to 4094.

port_ids
: Specifies the port ID. When specifying the DYNAMIC keyword, you can specify multiple port IDs. MAC addresses associated with the specified to the port ID are deleted. Use a comma (,) to separate port IDs and a hyphen (-) to indicate the range of port IDs.

macaddress
: Specifies the MAC address you want to delete from the switch's MAC address table. The address must be specified in the following format: xx:xx:xx:xx:xx:xx.

Mode

Privileged Exec mode

Description

Use this command to delete addresses from the MAC address table. You can delete MAC address entries listed in the Switching Forwarding Database section of the MAC address table. To display these MAC addresses, use the SHOW MAC ADDRESS TABLE command. See "SHOW MAC ADDRESS-TABLE" on page 394. To delete the Multicast Switch Forwarding Database section of the MAC address table, use the CLEAR IP IGMP command. See "CLEAR IP IGMP" on page 426

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 394.

Examples

This example deletes all of the dynamic addresses from the table:

```
awplus> enable
awplus# clear mac address-table dynamic
```

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 all of the static entries of the MAC addresses associated with port 1.0.10:

```
awplus> enable
awplus# clear mac address-table static interface port1.0.10
```

This example deletes all of the dynamic addresses learned on the ports of the VLAN with a VID of 12:

```
awplus> enable
awplus# clear mac address-table dynamic vlan 12
```

MAC ADDRESS-TABLE AGEING-TIME

Syntax

```
mac address-table ageing-time time
```

Parameter

time
: Specifies the aging timer in seconds for the MAC address table. The range is 0 to 1,048,575 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 entries of MAC addresses from the MAC address table. By setting the aging timer, you prevent the table from becoming full of inactive addresses. An address is considered inactive if no frames are sent to or received from the MAC addresses for the duration of the timer.

Setting the aging timer to 0 disables the timer. No dynamic MAC addresses are aged out and the table stops learning new addresses after reaching its maximum capacity.

To restore the default setting of 300 seconds, use the NO MAC ADDRESS-TABLE AGEING-TIME command.

Confirmation Command

“SHOW MAC ADDRESS-TABLE” on page 394.

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 entries of MAC addresses from the table:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table ageing-time 0
```

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_id vlan vid
```

Parameters

macaddress
: Specifies the MAC address you want to add to the switch's MAC address table. Multicast MAC addresses are not permitted. The address must be specified in the following format: xx:xx:xx:xx:xx:xx

forward
: Forwards frames containing the MAC address as a destination address.

discard
: Discards frames containing the MAC address as a destination address.

port_id
: Specifies the port ID from which the switch forwards frames containing the MAC address as a destination address.

vid
: Specifies the ID number of the VLAN that the node of the MAC address is a member of. The range is 1 to 4,094.

Mode

Global Configuration mode

Description

Use this command to add a MAC address to the switch's MAC address table statically. A static MAC address is never timed out from the MAC address table, even when the end node is inactive. With this command, you can add only one static MAC address at a time.

The forward and discard keywords specify whether the switch forwards or discards frames containing the specified MAC address as a destination address. When you specify the discard keyword, the switch discards frames containing the MAC address as a designation address and does not forward the frames from the port. However, you *must* specify the port_id parameter in this command.

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 394

Examples

This example adds the MAC address 00:00:f4:12:34:56 to port 1.0.4 in VLAN 10. The port forwards the packets from the specified node:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 00:00:f4:12:34:56
forward interface port1.0.4 vlan 10
```

This example adds the MAC address 00:A0:D2:18:1A:11 to port 1.0.7 in the default VLAN, which has a VID of 1. The port discards frames destined to the MAC address:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 00:A0:D2:18:1A:11
discard interface port1.0.7 vlan 1
```

NO MAC ADDRESS-TABLE STATIC

Syntax

```
no mac address-table static macaddress forward|discard
interface port_id vlan vid
```

Parameters

macaddress
: Specifies the MAC address. The address must be specified in the following format: xx:xx:xx:xx:xx:xx.

forward
: Forwards frames containing the MAC address as a destination address.

discard
: Discards frames containing the MAC address as a destination address.

port_id
: Specifies the port ID from that the switch forwards frames containing the MAC address as a destination address.

vid
: Specifies the ID number of the VLAN that the specified port is a member of. The range is 1 to 4,094.

Mode

Global Configuration mode

Description

Use this command to delete static entries of MAC addresses from the switch's MAC address table. You must enter all of the parameters to delete a MAC address entry from the table.

Confirmation Command

"SHOW MAC ADDRESS-TABLE" on page 394

Example

This example deletes a MAC address entry of 00:A0:D2:18:1A:11 associated with port 1.0.12 and the default VLAN:

```
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
```

SHOW MAC ADDRESS-TABLE

Syntax

`show mac address-table [interface` *port_ids*`]|[vlan` *vid*`]`

Parameters

port_ids

Specifies the port ID or multiple port IDs. MAC addresses associated with the specified to the port ID are listed. Use a comma (,) to separate port IDs and a hyphen (-) to indicate the range of port IDs.

vid

Specifies the VLAN ID. MAC addresses that belong to the VLAN are listed. The range is 1 to 4,094.

Modes

Privileged Exec mode

Description

Use this command to display the ageing timer as well as the unicast and multicast MAC addresses the switch has stored in the MAC address table. You may view all of the addresses in the table or only the addresses learned or specified on a particular port or VLAN. See Figure 63 for an example of the table.

```
Aging Interval: 300 second(s)

Switch Forwarding Database
Total Number of MAC Addresses: 4
------------------------------------------------------------------
VLAN   port    mac                fwd
------------------------------------------------------------------
2      1.0.7   00:00:00:00:00:01  Forward     dynamic
1      1.0.37  00:00:00:00:00:03  Forward     dynamic
1      po2     00:15:77:FF:00:10  Forward     dynamic
1      CPU     00:E0:0C:02:01:FD  Forward     static

Multicast Switch Forwarding Database
Total Number of MCAST FDB Addresses: 1
------------------------------------------------------------------
VLAN   mac                        Port Maps (U:Untagged T:Tagged)
------------------------------------------------------------------
1      01:00:5E:00:01:01 Dynamic  U:port1.0.9
                                  T:
```

Figure 63. SHOW MAC ADDRESS-TABLE Command

The fields are described in Table 64.

Table 64. SHOW MAC ADDRESS-TABLE Command - Unicast Addresses

Field	Description
Aging interval	Displays the value of the ageing timer.
Switch Forwarding Database Section:	
Total Number of MAC Address	Displays the number of MAC address entries in the unicast MAC address table.
VLAN	Displays the ID number of the VLAN that the port is a member of.
port	Displays the port ID where the address was learned or assigned. When the entry was assigned to the discard action, this field displays DROP.
mac	Displays the MAC address.
fwd	Displays whether the entry was assigned to forward or discard.
(unlabeled)	Displays whether the entry was statically added or dynamically learned.
Multicast Switch Forwarding Database Section:	
Total Number of MCAST FDB addresses	Displays the number of multicast address entries in the multicast forwarding database on the switch.
VLAN	Displays the ID number of the VLAN that the port is a member of.
mac	Displays the multicast MAC address.
(unlabeled)	Displays the type of the address. It always shows dynamic.
PortMaps	Displays the port ID and whether the port is tagged or untagged.

Examples

This example displays the entire MAC address table:

```
awplus# show mac address-table
```

This example displays the MAC addresses learned or added on port 1.0.1:

```
awplus# show mac address-table interface port1.0.1
```

Chapter 16

RRP Snooping Commands

The Router Redundancy Protocol (RRP) Snooping commands are summarized in Table 65.

Table 65. Address Resolution Protocol Commands

Command	Mode	Description
“IP RRP SNOOPING” on page 398	Global Configuration	Enables the RRP Snooping feature.
“SHOW IP RRP SNOOPING” on page 399	User Exec and Privileged Exec	Displays information about RRP Snooping.

IP RRP SNOOPING

Syntax

```
ip rrp snooping
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the RRP Snooping feature. You cannot enable RRP Snooping and a Spanning Tree Protocol, STP, RSTP, or MSTP, at the same time. When enabling RRP Snooping, disable the Spanning Tree Protocol using the NO SPANNING-TREE ENABLE command. See “SPANNING-TREE ENABLE” on page 360.

To disable the RRP Snooping feature, use the NO IP RRP SNOOPING command.

Confirmation Command

“SHOW IP RRP SNOOPING” on page 399

Example

This example enables the RRP Snooping feature on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip rrp snooping
```

SHOW IP RRP SNOOPING

Syntax

```
show ip rrp snooping
```

Parameters

None

Modes

Privileged Exec mode

Description

Use this command to display information about RRP Snooping. Figure 64 is an example of the command output.

```
RRP Snooping
-------------------------------------------------------------
Status .......................Enabled

  Vlan     Master    Virtual MAC Address   UpTime
  ------------------------------------------------------------
  1        1.0.5     00:00:5e:00:01:0a     0 days 00:00:12
-------------------------------------------------------------
```

Figure 64. SHOW IP RRP SNOOPING Command

The fields are described inTable 66.

Table 66. SHOW IP RRP SNOOPING Command

Field	Description
Status	Displays whether RRP Snooping is enabled or disabled.
Vlan	Displays the VLAN ID.
Master	Displays the port ID connected to the master router or the network of the master router.
Virtual MAC Address	Displays the virtual MAC address of the router.
UpTime	Displays the time that the current master router has been the master router.

Example

This example displays information about RRP Snooping:

```
awplus# show ip rrp snooping
```

Section III

IPv4 Management

This section contains the following chapters:

Chapter 17

IPv4 Management Address Commands

The IPv4 management address commands are summarized in Table 67.

Table 67. Management IP Address Commands

Command	Mode	Description
“IP ADDRESS” on page 404	VLAN Interface	Assigns the switch a static IPv4 management address.
“IP ADDRESS DHCP” on page 406	VLAN Interface	Assigns the switch an IPv4 management address from a DHCP server on your network.
“IP ROUTE” on page 408	Global Configuration	Assigns the switch an IPv4 default gateway address.
“NO IP ADDRESS” on page 409	VLAN Interface	Deletes the IPv4 management address.
“NO IP ROUTE” on page 410	Global Configuration	Deletes the IPv4 default gateway.
“PING” on page 411	Privileged Exec	Instructs the switch to ping another network device.
“SHOW IP INTERFACE” on page 412	Privileged Exec	Displays the IPv4 management address.
“SHOW IP ROUTE” on page 413	Privileged Exec	Displays the IPv4 management address and default gateway.

IP ADDRESS

Syntax

`ip address` *`ipaddress/mask`*

Parameters

`ipaddress`
Specifies a management IPv4 address for the switch.

`mask`
Specifies the subnet mask for the address.

Mode

VLAN Interface mode

Description

Use this command to manually assign an IPv4 management address to an VLAN interface and the management Ethernet port eth0. You can assign one IPv4 address for one VLAN and one IPv4 address for the eth0 port.

The two IPv4 management addresses, assigned to a VLAN interface and the management Ethernet port eth0, must be IPv4 addresses that belong to *different* networks. For example, if you assign 192.168.2.10/24 to VLAN 1, you cannot assign any addresses in the 192.168.2.0/24 network to the eth0 port.

When you want to change the IPv4 address assignment, you must delete the IPv4 address using the NO IP ADDRESS command and reassign a new IPv4 address. See “NO IP ADDRESS” on page 409.

To assign the switch an IPv4 address from a DHCP server, refer to “IP ADDRESS DHCP” on page 406.

Confirmation Command

“SHOW IP INTERFACE” on page 412

Example

This example assigns the switch the IPv4 management address 192.168.10.1 and a subnet mask of 255.255.255.0. The address is assigned to the Default_VLAN, which has a VID of 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-vlan)# ip address 192.168.10.1/24
```

IP ADDRESS DHCP

Syntax

```
ip address dhcp [client-id client_id] [hostname hostname]
```

Parameters

client_id
: Specifies the name of the VLAN interface. This parameter is set to the client ID (option code: 61) for DHCP Discovery and Request messages.

hostname
: Specifies a hostname. This parameter is set to the host name (option code: 12) for DHCP Discovery and Request messages. The host name can be up to 39 alphanumeric characters.

Mode

VLAN Interface mode

Description

Use this command to assign an IPv4 management address from a DHCP server to the VLAN interface and management Ethernet port eth0. The command activates the DHCP client, which automatically queries the network for a DHCP server and obtains an IP address from the DHCP server. The client also queries for a DHCP server and obtains an IP address whenever you reset or power cycle the switch.

To add a client ID and host name to DHCP Discovery and Request messages, use this command with the client-id and host name parameters.

You can assign one IPv4 address to one VLAN and one IPv4 address to the eth0 port. When using this command for the eth0 port, you cannot specify the client-id and hostname parameters.

You can delete the assigned IPv4 address using the NO IP ADDRESS or NO IP ADDRESS DHCP command.

Confirmation Commands

“SHOW IP INTERFACE” on page 412 and “SHOW IP ROUTE” on page 413

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 a VID of 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-vlan)# ip address dhcp
```

IP ROUTE

Syntax

```
ip route 0.0.0.0/0 ipaddress
```

Parameter

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 can have only *one* default gateway 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.

Confirmation Command

"SHOW IP ROUTE" on page 413

Example

This example assigns the switch the IPv4 default gateway address of 192.168.1.32:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip route 0.0.0.0/0 192.168.1.32
```

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 a VLAN interface or management Ethernet port eth0. In addition, you can use this command to delete an IPv4 management address assigned with the IP ADDRESS DHCP command.

Confirmation Commands

"SHOW IP INTERFACE" on page 412 and "SHOW IP ROUTE" on page 413

Example

This example removes the static IPv4 management address from the VLAN with the VID 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-vlan)# no ip address
```

NO IP ROUTE

Syntax

```
no ip route 0.0.0.0/0 ipaddress
```

Parameter

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 413

Example

This example deletes the default gateway 192.168.1.32 from the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip route 0.0.0.0/0 192.168.1.32
```

PING

Syntax

```
ping ipaddress
```

Parameter

ipaddress
: Specifies the IPv4 address of the network device. You can specify only one IP address.

Modes

Privileged Exec mode

Description

Use this command to instruct the switch to send ICMP Echo Requests to a network device with the IPv4 address specified. You may want to use the command to determine whether an active link is available between the switch and another network device.

Example

This command instructs the switch to ping a network device with an IP address of 192.168.1.32

```
awplus> enable
awplus# ping 192.168.1.32
```

The results of the ping are displayed on the screen.

SHOW IP INTERFACE

Syntax

```
show ip interface
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the management IPv4 address on the switch. See Figure 65 for an example of the information.

```
Interface      IP-Address          Status        Protocol
eth0           192.168.1.1/24      admin up      running
VLAN1-0        192.168.10.1/24     admin up      down
```

Figure 65. SHOW IP INTERFACE Command

The fields are described in Table 68.

Table 68. SHOW IP INTERFACE Command

Field	Description
Interface	Displays the name of the interface to which the management IP address is assigned. A VLAN interface is displayed with the “-0” suffix.
IP Address	Displays the IPv4 management address and subnet.
Status	Displays the management status of the interface as up or down.
Protocol	Displays the link status of the interface as running or down.

Example

This example displays the management IPv4 address on the 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 IP routing table on the switch. See Figure 66 for an example of the command output.

```
-------------------------------------------------------------------
Destination    Mask            NextHop          Interface  Protocol
-------------------------------------------------------------------
192.168.1.0    255.255.255.0   192.168.1.1      eth0       INTERFACE
192.168.10.0   255.255.255.0   192.168.10.1     vlan1-0    INTERFACE
0.0.0.0        0.0.0.0         192.168.1.32     eth0       STATIC
```

Figure 66. SHOW IP ROUTE Command

The fields are described in Table 69.

Table 69. SHOW IP ROUTE Command

Field	Description
Destination	Displays the network address of the destination.
Mask	Displays the subnet mask of the destination network address.
NextHop	Displays the next hop address.
Interface	The VID of the VLAN to which the management IP address is assigned.

Table 69. SHOW IP ROUTE Command (Continued)

Field	Description
Protocol	Indicates the source of the routing information. The options are: ❒ INTERFACE: The route is based on the IP address that is assigned statically to the interface. ❒ STATIC: The route is assigned statically. ❒ DHCP: The route is based on the IP address or default gateway address that is assigned by a DHCP server.

Example

This example displays the IP routing table on the switch:

```
awplus# show ip route
```

Chapter 18
ARP Commands

The ARP commands are summarized in Table 70.

Table 70. Address Resolution Protocol Commands

Command	Mode	Description
“ARP” on page 416	Global Configuration	Adds static ARP entries to the ARP cache.
“ARP TIMEOUT” on page 417	Global Configuration	Changes the ARP timeout value.
“CLEAR ARP-CACHE” on page 418	Global Configuration	Deletes all dynamic ARP entries from the ARP cache.
“NO ARP” on page 419	Global Configuration	Deletes a static ARP entry from the ARP cache.
“SHOW ARP” on page 420	User Exec and Privileged Exec	Displays the static and dynamic ARP entries in the ARP cache.

ARP

Syntax

arp *ipaddress macaddress port_id*

Parameters

ipaddress
Specifies the IPv4 address of the host.

macaddress
Specifies the MAC address of the host. The MAC address must be entered in the hexadecimal format:

port_id
Specifies the ID of the port connected to the host. The port must be a member of the VLAN that has an assigned IPv4 management address.

Mode

Global Configuration mode

Description

Use this command to add a static ARP entry to the ARP cache on the switch. You add entries for local hosts that do not support ARP or to speed up the address resolution function for a host.

Confirmation Command

“SHOW ARP” on page 420

Example

This example creates an ARP entry for the IP address 192.168.10.254 and the MAC address 7A:54:2B:11:65:72 on port 1.0.25:

```
awplus> enable
awplus# configure terminal
awplus(config)# arp 192.168.10.254 7a:54:2b:11:65:72
port1.0.25
```

ARP TIMEOUT

Syntax

```
arp timeout time
```

Parameter

time

Specifies the ARP timeout value, in seconds, that the switch retains an ARP entry in the ARP cache. The range is 60 to 260,000 seconds. By default, the ARP timeout is 300 seconds.

Mode

Global Configuration mode

Description

Use this command to change the ARP timeout value. The switch deletes an ARP entry after the ARP entry times out unless the switch receives a frame from the MAC address.

To restore the ARP timeout value to the default of 300 seconds, use the NO ARP TIMEOUT command.

Confirmation Command

"SHOW ARP" on page 420

Examples

This example changes the ARP timeout to 600 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# arp timeout 600
```

This example changes the ARP timeout to the default of 300 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no arp timeout
```

CLEAR ARP-CACHE

Syntax

```
clear arp-cache
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to delete all dynamic ARP entries from the ARP cache. To delete a static ARP entry, use the NO ARP command. See “NO ARP” on page 419.

Confirmation Command

“SHOW ARP” on page 420

Example

This example deletes all dynamic ARP entries from the ARP cache:

```
awplus> enable
awplus# configure terminal
awplus(config)# clear arp-cache
```

NO ARP

Syntax

```
no arp ipaddress
```

Parameter

ipaddress
Specifies the IP address of the host.

Mode

Global Configuration mode

Description

Use this command to delete a static ARP entry from the ARP cache by specifying the IP address of the host. This command can delete only one ARP entry at a time.

Confirmation Command

"SHOW ARP" on page 420

Example

This example deletes the ARP entry for the IP address 192.168.10.254:

```
awplus> enable
awplus# configure terminal
awplus(config)# no arp 192.168.10.254
```

SHOW ARP

Syntax

```
show arp
```

Parameters

None

Modes

User Exec mode and Privileged Exec mode

Description

Use this command to display the entries in the ARP cache. The ARP cache contains mappings of IP addresses to physical addresses for hosts where the switch has recently forwarded packets. See Figure 67 for an example of the information displayed by this command.

```
IP ARP
ARP Cache Timeout ......... 300 seconds
Total ARP Entries ......... 4
------------------------------------------------------------------

IP Address      MAC Address          Interface  Port         Type
192.168.1.1     00:06:5b:88:80:4     eth0                    Dynamic
192.168.10.2    00:22:19:d4:4c:7a    vlan1-0    port1.0.1    Dynamic
192.168.10.32   00:00:cd:37:07:e4    vlan1-0    port1.0.3    Dynamic
192.168.10.70   00:24:e8:08:ad:ab    vlan1-0    port1.0.11   Dynamic
```

Figure 67. SHOW ARP Command

The fields are described inTable 71.

Table 71. SHOW ARP Command

Field	Description
ARP Cache Timeout	Displays the ARP timeout value that an ARP remains in the ARP cache
Total ARP Entries	Displays the number of ARP entries on the switch.
IP Address	Displays the IP address of the node.
MAC Address	Displays the MAC address of the node.

Table 71. SHOW ARP Command (Continued)

Field	Description
Interface	Displays the VLAN ID with the suffix "-0"
Port	Displays the port ID from where the host is connected.
Type	Displays the type of the entry. The options are: ❒ Static: Indicates a static entry added with "ARP" on page 416. ❒ Dynamic: Indicates an entry learned from ARP request and reply exchanges.

Example

This example displays the entries in the ARP cache:

```
awplus# show arp
```

Section IV

IPv4 Multicast

This section contains the following chapter:

Chapter 19

IGMP Snooping Commands

The IGMP snooping commands are summarized in Table 72.

Table 72. Internet Group Management Protocol Snooping Commands

Command	Mode	Description
“CLEAR IP IGMP” on page 426	Privileged Exec	Clears all IGMP group membership records.
“IP IGMP LIMIT” on page 427	Global Configuration	Specifies the maximum number of multicast addresses the switch can register.
“IP IGMP QUERIER-TIMEOUT” on page 428	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 429	Global Configuration	Enables IGMP snooping on the switch.
“IP IGMP SNOOPING MROUTER INTERFACE” on page 430	Global Configuration	Manually identifies the ports where multicast routers are connected.
“IP IGMP STATUS” on page 431	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 432	Global Configuration	Disables IGMP snooping on the switch.
“NO IP IGMP SNOOPING MROUTER INTERFACE” on page 433	Global Configuration	Removes multicast router ports.
“SHOW IP IGMP” on page 434	Privileged Exec	Displays the IGMP snooping configuration on the switch.
“SHOW IP IGMP HOSTLIST” on page 435	Privileged Exec	Displays the multicast router list on the switch.
“SHOW IP IGMP MROUTER” on page 436	Privileged Exec	Displays the IGMP host list on the switch.
“SHOW IP IGMP SNOOPING” on page 437	Privileged Exec	Displays the IGMP snooping configuration, multicast router list, and host list on the switch.

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.

Confirmation Command

“SHOW IP IGMP SNOOPING” on page 437

Example

This example deletes all IGMP group membership records on the switch:

```
awplus> enable
awplus# clear ip igmp
```

IP IGMP LIMIT

Syntax

```
ip igmp limit multicastgroups
```

Parameter

multicastgroups
: Specifies the maximum number of multicast groups that the switch can register. The range is 0 to 255 multicast groups. By default, the value is 64 groups.

Mode

Global Configuration mode

Description

Use this command to specify the maximum number of multicast groups that the switch is permitted to store.

Confirmation Command

"SHOW IP IGMP" on page 434

Example

This example sets the maximum number of multicast groups on the switch to 132:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp limit 132
```

IP IGMP QUERIER-TIMEOUT

Syntax

```
ip igmp querier-timeout timeout
```

Parameter

timeout
: Specifies the time period, in seconds, used by the switch to delete host entries and multicast router entries when they time out. The range is from 0 to 86,400 seconds (24 hours). The default is 260 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 delete host and multicast router entries. The time period is in seconds.

A host node multicast router is deemed inactive and its entries on the switch are deleted if the switch does not receive IGMP reports or queries from the host or router for the duration of the timer.

Confirmation Command

“SHOW IP IGMP” on page 434

Example

This example sets the timeout for host entries and multicast router entries 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 enable IGMP snooping on the switch. IGMP snooping allows the switch to examine the contents of packets (sent between hosts and routers) and filter multicast packets. Without IGMP, the switch floods multicast packets to all the hosts that belong to a VLAN even if only one host in the VLAN is a recipient of the multicast packet. By default, IGMP snooping is enabled.

When IGMP snooping is enabled, the switch does not apply hardware ACLs and policy maps to IGMP packets.

The switch supports jumbo frames up to 12,292 bytes; however, when IGMP snooping is enabled, the ports discard:

- Frames with VLAN tags larger than 1,518 bytes
- Frames without VLAN tags larger than 1,522 bytes

Confirmation Command

"SHOW IP IGMP" on page 434

Example

This example enables IGMP snooping on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping
```

IP IGMP SNOOPING MROUTER INTERFACE

Syntax

```
ip igmp snooping mrouter interface port_ids
```

Parameter

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

Global Configuration mode

Description

Use this command to manually specify ports that are connected to multicast routers. To specify a trunk group, specify the individual port members of a trunk group instead of port trunk IDs. For example, if the port trunk “sa1” consists of ports 1.0.1 to 1.0.5, specify member ports “port1.0.1-port1.0.5” instead of “sa1.”

To reactivate auto-detect, remove all static multicast router ports. See “NO IP IGMP SNOOPING MROUTER INTERFACE” on page 433.

Confirmation Command

“SHOW IP IGMP” on page 434

Example

This example identifies ports 1.0.14 and 1.0.15 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. Each port on the switch has only one host. This is the default setting.

`multiple`
: Activates the multiple-host per port setting. A port on the switch can have multiple hosts.

Mode

Global Configuration mode

Description

Use this command to specify the IGMP host node topology as single or multiple host per port. When receiving IGMP leave messages, the switch responds depending on the IGMP host node topology specified.

Confirmation Command

"SHOW IP IGMP" on page 434

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 disable IGMP snooping on the switch.

Confirmation Command

“SHOW IP IGMP” on page 434

Example

This example disables IGMP snooping on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping
```

NO IP IGMP SNOOPING MROUTER INTERFACE

Syntax

```
no ip igmp snooping mrouter interface port_ids
```

Parameter

port_ids
: Specifies a multicast router port ID or multiple port IDs to delete. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

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" on page 434

Example

This example removes port 1.0.3 as multicast router ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping mrouter interface
port1.0.3
```

SHOW IP IGMP

Syntax

```
show ip igmp
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the IGMP snooping configuration on the switch. See Figure 68 for an example of the command output.

```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Enabled
  Host Topology ...................... Single-Host/Port
  Host/Router Timeout Interval ....... 260 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect
```

Figure 68. SHOW IP IGMP Command

The fields are described in the SHOW IP IGMP SNOOPING command table. See the IGMP Snooping Configuration section of Table 73 on page 438.

Example

This example displays the IGMP snooping configuration on the switch:

```
awplus# show ip igmp
```

SHOW IP IGMP HOSTLIST

Syntax

```
show ip igmp hostlist
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the IGMP host list. See Figure 69 for an example of the command output.

```
Host List:
Number of IGMP Multicast Groups: 1

                VLAN   Port/                      IGMP    Exp.
MultcastGroup   ID     TrunkID    HostIP          Ver     Time
-------------------------------------------------------------
224.0.1.1       1      port1.0.3  192.168.1.100    v2     228
```

Figure 69. SHOW IP IGMP HOSTLIST Command

The fields are described in the SHOW IP IGMP SNOOPING command table. See the Host List section of Table 73 on page 438.

Example

This example displays the IGMP host list:

```
awplus# show ip igmp hostlist
```

SHOW IP IGMP MROUTER

Syntax

```
show ip igmp mrouter
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display information about the IGMP multicast routers. See Figure 70 for an example of this information.

```
Router List:

VLAN   Port/                          Exp.
ID     Trunk ID     RouterIP          Time
-------------------------------------------------
1      port1.0.3    192.168.1.10      255
```

Figure 70. SHOW IP IGMP MROUTNER Command

The fields are described in the SHOW IP IGMP SNOOPING command table. See the Router List section of Table 73 on page 438.

Example

This example displays information about the IGMP multicast routers:

```
awplus# show ip igmp mrouter
```

SHOW IP IGMP SNOOPING

Syntax

```
show ip igmp snooping
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the IGMP snooping configuration, multicast router list, and host list. See Figure 71 for an example of the command output.

```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Enabled
  Host Topology ...................... Single-Host/Port
  Host/Router Timeout Interval ....... 260 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect

Router List:

VLAN   Port/                          Exp.
       ID          Trunk ID           RouterIP Time
-------------------------------------------------
1      port1.0.3   192.168.1.10       228

Host List:
Number of IGMP Multicast Groups: 1

                 VLAN   Port/                      IGMP   Exp.
MultcastGroup    ID     TrunkID    HostIP          Ver    Time
-----------------------------------------------------------
224.0.1.1        1      port1.0.3  192.168.1.100   v2     230
```

Figure 71. SHOW IP IGMP SNOOPING Command

The fields are described in Table 73.

Table 73. SHOW IP IGMP SNOOPING Command

Field	Description
IGMP Snooping Configuration:	
IGMP Snooping Status	Displays the status of IGMP snooping on the switch. The options are: ❒ Enabled ❒ Disabled To enable IGMP snooping, refer to See “IP IGMP SNOOPING” on page 429.
Host Topology	Displays the IGMP host node topology on the switch specified by the IP IGMP STATUS command. The options are: ❒ Single-Host - Each port has only one host. ❒ Multi-Hosts - Each port can have more than one host node. To set the IGMP host node topology, refer to See “IP IGMP STATUS” on page 431.
Host/Router Timeout Interval	Displays 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 428.
Maximum IGMP Multicast Groups	Displays the maximum number of multicast groups the switch supports. This number is specified by the IP IGMP LIMIT command. Refer to “IP IGMP LIMIT” on page 427.
Router Port(s)	Displays the ports connected to multicast routers. If you do not manually assign multicast router ports using the IP IGMP SNOOPING MROUTER INTERFACE command, this field displays “Auto Detect.” Refer to “IP IGMP SNOOPING MROUTER INTERFACE” on page 430.
Router List:	
VLAN ID	Displays the ID number of the VLAN of the router ports.

Table 73. SHOW IP IGMP SNOOPING Command (Continued)

Field	Description
Port/TrunkID	Displays the port ID of a multicast router. If the switch learned a router on a port trunk, the trunk ID number instead of a port ID number is displayed.
RouterIP	Displays the IP addresses of the multicast router.
Exp. Time	Displays the number of seconds remaining before the switch times out the entry. Refer to "IP IGMP QUERIER-TIMEOUT" on page 428.
Host List:	
Number of IGMP Multicast Groups	Displays the number of IGMP multicast groups on the switch. Refer to "IP IGMP LIMIT" on page 427.
Multicast Group	Displays the multicast addresses of the groups.
VLAN ID	Displays the ID number of the VLAN that a port or trunk group connected to a multicast recipient host is a member of.
Port/Trunk ID	Displays the port or of trunk group where multicast recipient hosts are connected. If the host nodes are on port trunks, this field displays the trunk ID numbers instead of the port numbers.
HostIP	Displays the IP addresses of the host nodes
IGMP Ver	Displays the IGMP version.
Exp. Time	Displays the number of seconds remaining before the switch times out the entry.

Example

This example displays the IGMP snooping configuration, multicast router list, and host list:

```
awplus# show ip igmp snooping
```

Section V

Security and Traffic Control

This section contains the following chapters:

Chapter 20

ACL Commands

The Access Control List (ACL) commands are summarized in Table 74.

Table 74. Access Control List Commands

Command	Mode	Description
“ACCESS-GROUP” on page 445	Port Interface	Assigns hardware access control lists to ports.
“ACCESS-LIST HARDWARE” on page 447	Global Configuration	Creates a new hardware access list or modifies an existing hardware access list.
“COPY-TO-MIRROR” on page 448	Hardware Access List	Adds a new copy-to-mirror statement to the hardware access control list or modifies an existing copy-to-mirror statement.
“DENY” on page 453	Hardware Access List	Adds a new deny statement to the hardware access control list or modifies an existing deny statement.
“NO ACCESS-GROUP” on page 458	Port Interface	Removes the assignment of a hardware access control list to the switch port.
“NO ACCESS-LIST HARDWARE” on page 459	Global Configuration	Deletes hardware access lists from the switch.
“NO COPY-TO-MIRROR” on page 460	Hardware Access List	Deletes a copy-to-mirror statement from the hardware access control list.
“NO DENY” on page 463	Hardware Access List	Deletes a deny statement from the hardware access control list.
“NO PERMIT” on page 466	Hardware Access List	Deletes a permit statement from the hardware access control list.
“PERMIT” on page 469	Hardware Access List	Adds a new permit statement to the hardware access control list or modifies an existing permit statement.
“SHOW ACCESS-LIST” on page 474	Privileged Exec	Displays the ACLs on the switch.
“SHOW INTERFACE ACCESS-GROUP” on page 475	Privileged Exec	Displays the port assignments of the hardware access control lists.

Table 74. Access Control List Commands (Continued)

Command	Mode	Description
“SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION” on page 476	Privileged Exec	Displays the consumption of the memory on the switching chip that is allocated to DoC, ACL, and QoS functions.

ACCESS-GROUP

Syntax

```
access-group acl_name
```

Parameter

acl_name
: Specifies the name of a hardware access control list to assign to the switch port.

Mode

Port Interface mode

Description

Use this command to assign a hardware Access Control List (ACL) to switch ports.

When a switch port receives packets, the switch evaluates them against each statement in the hardware ACLs assigned to the port. When a packet matches a statement, the switch takes an action listed in the statement and skips the rest of the statements. If a packet does not match any statements, the switch forwards the packet.

Here are guidelines for applying hardware ACLs:

- You can assign up to 256 hardware ACLs to a switch port; however, the number of ACLs the switch process depends on the available memory of the switching chip allocated to the ACL function.
- When IGMP Snooping is enabled on a switch port, the switch does not evaluate hardware access control lists assigned to the switch port. IGMP Snooping is enabled by default.
- When a switch port is assigned policy maps and Denial of Service (DoS) statements as well as ACLs, the switch evaluates received packets on the switchport against DoS statements, ACL, and policy maps in this order.
- When assigning hardware ACLs to a trunk group (saX and poX), assign them to ports. Assigning hardware ACLs to a trunk group is *not* permitted.

Confirmation Command

"SHOW INTERFACE ACCESS-GROUP" on page 475

Example

This example assigns the hardware access control list acl_10 to ports1.0.15 through 1.0.20:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15-port1.0.20
awplus(config-if)# access-group acl_10
```

ACCESS-LIST HARDWARE

Syntax

```
access-list hardware acl_name
```

Parameter

acl_name
: Specifies the name of an ACL. The name is case-sensitive and can contain up to 63 alphanumeric characters. Spaces, exclamation marks (!), and question marks (?) are *not* permitted.

Mode

Global Configuration mode

Description

Use this command to create or modify a hardware ACL and enter the Hardware Access List mode. You can create up to 512 hardware access lists per switch.

Note
When a hardware ACL is used for a class map, you cannot modify the hardware ACL.

Confirmation Command

"SHOW ACCESS-LIST" on page 474

Examples

This example creates a new hardware access list named "acl_5":

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_5
awplus(config-ip-hw-acl)#
```

This example moves the command mode to the Hardware Access List mode to modify the existing access list "acl_1":

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_1
awplus(config-ip-hw-acl)#
```

COPY-TO-MIRROR

Syntaxes

[*sequence_no*] copy-to-mirror mac *src_mac_address wildcard_mask*|any *dst_mac_address wildcard_mask*|any [vlan *vid*]

[*sequence_no*] copy-to-mirror ip *src_ip_address/mask*|host *src_ip_address*|any *dst_ip_address/mask*|host *dst_ip_address*|any [mac *src_mac_address wildcard_mask*|any *dst_mac_address wildcard_mask*|any] [vlan *vid*]

[*sequence_no*] copy-to-mirror proto *proto_no* *src_ip_address/mask*|host *src_ip_address*|any *dst_ip_address/mask*|host *dst_ip_address*|any [*mac src_mac_address wildcard_mask*|any *dst_mac_address wildcard_mask*|any] [vlan *vid*]

[*sequence_no*] copy-to-mirror icmp *src_ip_address/mask*|host *src_ip_address*|any *dst_ip_address/mask*|host *dst_ip_address*|any [icmp *icmp_type*] [vlan *vid*]

[*sequence_no*] copy-to-mirror tcp|udp *src_ip_address/mask*|host *src_ip_address*|any [*src_port_no*] *dst_ip_address/mask*|host *dst_ip_address*|any [*dst_port_no*] [vlan *vid*]

Parameters

sequence_no

Specifies a sequence number. The sequence number determines the place of the entry in the access list. When you specify an existing sequence number, the command replaces it with the new definition. If you do not specify a sequence number, the command adds the entry to the end of the access list. The range of the sequence numbers is 1 to 65,535.

src_mac_address

Specifies a source MAC address that the switch uses to filter packets. This is the hexadecimal format:

HH:HH:HH:HH:HH:HH

dst_mac_address

Specifies a destination MAC address that the switch uses to filter packets. The format is the same as the source MAC address.

wildcard_mask

Specifies a wildcard mask for the MAC address. The wildcard mask determines how much of a MAC address to apply to the MAC address match. This is the hexadecimal format:

XX:XX:XX:XX:XX:XX

The "X" variable can be "0" or "F." Use the wildcard mask value "0" for parts of the MAC address that the switch uses to filter on. Use the wildcard mask value "F" for parts of the MAC address that the switch ignores. Specify a wildcard mask of 00:00:00:00:00:00 when you want the switch match the exact MAC address that you specify.

`any`

Specifies that any MAC addresses or IP addresses are used for filtering.

vid

Specifies the VLAN ID of a receiving packet that the switch filters on. Enter a value from 1 to 4,094.

src_ip_address

Specifies a source IPv4 address that the switch filters packets on.

dst_ip_address

Specifies a destination IPv4 address that the switch filters packets on.

mask

Specifies a mask that determines the number of bits of an IP address to apply to the IP address match.

`host`

Specifies the host keyword and an IPv4 address when you want the switch to match the exact IPv4 address that you specify. The host keyword and an IPv4 address is equivalent to an IPv4 address with a mask of 32.

proto_no

Specifies the value of a protocol field in a packet that the switch filters on.The range is 1 to 255.

icmp_type

Specifies an ICMP message type. If you do not specify an ICMP message type, the switch does not filter packets based on an ICMP message type. The options are:

0: Echo Reply

3: Destination Unreachable

4: Source Quench

5: Redirect

8: Echo Request

9: Router Advertisement

10: Router Solicitation

11: Time Exceeded

12: Parameter Problem

13: Timestamp

14: Timestamp Reply

15: Information Request

16: Information Reply

17: Address Mask Request

18: Address Mask Replay

src_port_no

Specifies source TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the following formulas:

– eq *src_port_no*: Matches a packets whose port number is equal to the specified port number.

– lt *src_port_no*: Matches packets whose port number is less than the specified port number.

– gt *src_port_no*: Matches packets whose port number is greater than the specified port number.

– ne *src_port_no*: Matches a packet whose port number is not equal to the specified port number.

– range *src_port_no src_port_no*: Matches packets whose port number is within the range.

dst_port_no

Specifies destination TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the formulas described in the *src_port_no* parameter.

Mode

Hardware Access List mode

Confirmation Command

"SHOW ACCESS-LIST" on page 474

Description

Use this command to add a new copy-to-mirror statement to the hardware ACL or modify an existing copy-to-mirror statement. When a packet matches a copy-to-mirror statement, the switch forwards the packet, copies the packet, and sends it to the mirror port. You can add up to 256 statements to one hardware ACL. To specify the mirror port, see "MIRROR INTERFACE" command.

The hardware access list is a sequential collection of permit, deny, or copy-to-mirror statements. The switch evaluates a packet against the statement one by one from the smallest sequence number to the largest. When a packet matches the statement, the switch permits, denies, or mirrors the packet and skips the rest of the statements. If a packet does not match any statements, the switch forwards the packet.

To add or modify a permit or deny statement, see "PERMIT" on page 469 or "DENY" on page 453.

Examples

This example creates a new hardware access list named "acl_1" and adds a statement to forward packets and copy them to the mirror port when the prefix of a source MAC address in the packets is "ec:cd:6d":

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_1
awplus(config-ip-hw-acl)# copy-to-mirror mac
ec:cd:6d:00:00:00 00:00:00:ff:ff:ff any
```

This example selects an existing hardware access list named "acl_2" and adds a statement at the end of the acl_2 to forward packets and copy them to the mirror port when packets have destination IP addresses of 192.168.1.0./24 and belong to VLAN 10:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_2
awplus(config-ip-hw-acl)# copy-to-mirror ip any 192.168.1.0/
24 vlan 10
```

This example creates a new hardware access list named “acl_3” and adds a statement to forward packets and copy them to the mirror port when packets have a protocol type of TCP, a source IP address of 192.168.10.5, and a TCP port number of 80:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_3
awplus(config-ip-hw-acl)# copy-to-mirror tcp host
192.168.10.5 any eq 80
```

DENY

Syntaxes

[*sequence_no*] deny mac *src_mac_address wildcard_mask*|any *dst_mac_address wildcard_mask*|any [vlan *vid*]

[*sequence_no*] deny ip *src_ip_address/mask*|host *src_ip_address*|any *dst_ip_address/mask*|host *dst_ip_address*|any [*mac src_mac_address wildcard_mask*|any *dst_mac_address wildcard_mask*|any] [vlan *vid*]

[*sequence_no*] deny proto *proto_no* *src_ip_address/mask*|host *src_ip_address*|any *dst_ip_address/mask*|host *dst_ip_address*|any [*mac src_mac_address wildcard_mask*|any *dst_mac_address wildcard_mask*|any] [vlan *vid*]

[*sequence_no*] deny icmp *src_ip_address/mask*|host *src_ip_address*|any *dst_ip_address/mask*|host *dst_ip_address*|any [icmp *icmp_type*] [vlan *vid*]

[*sequence_no*] deny tcp|udp *src_ip_address/mask*|host *src_ip_address*|any [*src_port_no*] *dst_ip_address/mask*|host *dst_ip_address*|any [*dst_port_no*] [vlan *vid*]

Parameters

sequence_no

Specifies a sequence number. The sequence number determines the place of the entry in the access list. When you specify an existing sequence number, the command replaces it with the new definition. If you do not specify a sequence number, the command adds the entry to the end of the access list. The range of the sequence numbers is 1 to 65,535.

src_mac_address

Specifies a source MAC address. This is the hexadecimal format:

HH:HH:HH:HH:HH:HH

dst_mac_address

Specifies a destination MAC address that the switch filters packets based on. The format is the same as the source MAC address.

wildcard_mask
: Specifies a wildcard mask for the MAC address. The wildcard mask determines how much of a MAC address to apply to the MAC address match. This is the hexadecimal format:

  XX:XX:XX:XX:XX:XX

  The “X” variable can be “0” or “F.” Use the wildcard mask value “0” for parts of the MAC address that the switch uses to filter on. Use the wildcard mask value “F” for parts of the MAC address that the switch ignores. Specify a wildcard mask of 00:00:00:00:00:00 when you want the switch match the exact MAC address that you specify.

any
: Specifies that any MAC addresses or IP addresses are used for filtering.

vid
: Specifies the VLAN ID of a receiving packet that the switch filters on. Enter a value between 1 and 4,094.

src_ip_address
: Specifies a source IPv4 address that the switch filters packets on.

dst_ip_address
: Specifies a destination IPv4 address that the switch filters packets on.

mask
: Specifies a mask that determines how many bits of an IP address to apply to the IP address match.

host
: Specifies the host keyword and an IPv4 address when you want the switch match the exact IPv4 address that you specify. The host keyword in combination with an IPv4 address is equivalent to an IPv4 address with a mask of 32.

proto_no
: Specifies the value of a protocol field in a packet that the switch filters on.The range is 1 to 255.

icmp_type
: Specifies an ICMP message type. When you do not specify an ICMP message type, the switch does not filter packets based on an ICMP message type. The options are:

  0: Echo Reply

  3: Destination Unreachable

4: Source Quench

5: Redirect

8: Echo Request

9: Router Advertisement

10: Router Solicitation

11: Time Exceeded

12: Parameter Problem

13: Timestamp

14: Timestamp Reply

15: Information Request

16: Information Reply

17: Address Mask Request

18: Address Mask Replay

src_port_no

Specifies source TCP or UDP port numbers. The range is 0 to 65535. To specify port numbers, use one of the following formulas:

– eq *src_port_no*: Matches a packets whose port number is equal to the specified port number.

– lt *src_port_no*: Matches packets whose port number is less than the specified port number.

– gt *src_port_no*: Matches packets whose port number is greater than the specified port number.

– ne *src_port_no*: Matches a packet whose port number is not equal to the specified port number.

– range *src_port_no src_port_no*: Matches packets whose port number is within the range.

dst_port_no

Specifies destination TCP or UDP port numbers. The range is 0 to 65535. To specify port numbers, use one of the formulas described in the *src_port_no* parameter.

Mode

Hardware Access List mode

Description

Use this command to add a deny statement to the hardware ACL or modify an existing deny statement. When a packet matches a deny statement, the switch discards the packet. You can add up to 256 statements to one hardware ACL.

The hardware ACL is a sequential collection of permit, deny, or copy-to-mirror statements. The switch evaluates a packet against the statement one by one from the smallest sequence number to the largest. When a packet matches the statement, the switch permits, denies, or copies to mirror the packet and skips the rest of the statements. If a packet does not match any statements, the switch forwards the packet.

To add or modify a permit or copy-to-mirror statement, see “PERMIT” on page 469 or “COPY-TO-MIRROR” on page 448

Confirmation Command

“SHOW ACCESS-LIST” on page 474

Examples

This example creates a new hardware ACL named “acl_1” and adds a statement to discard packets when the prefix of a source MAC address in the packets is “ec:cd:6d”:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_1
awplus(config-ip-hw-acl)# deny mac ec:cd:6d:00:00:00
00:00:00:ff:ff:ff any
```

This example selects a new hardware ACL named “acl_2” and adds a statement at the end of “acl_2” to discard IP packets that have destination IP addresses of 192.168.1.0./24 and belong to VLAN 10:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_2
awplus(config-ip-hw-acl)# deny ip any 192.168.1.0/24 vlan 10
```

This example creates a new hardware access list named “acl_3” and adds a statement to discard packets that have a protocol type of TCP, a source IP address of 192.168.10.5, and a TCP port number of 80:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_3
awplus(config-ip-hw-acl)# deny tcp host 192.168.10.5 any eq
80
```

This example creates a new hardware access list named "acl_4" and adds a statement to discard packets from hosts in the 192.168.20.0/24 network who try to ping the host with the 192.168.10.1 address:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_3
awplus(config-ip-hw-acl)# deny icmp 192.168.20.0/24
192.168.10.1/32 icmp-type 8
```

NO ACCESS-GROUP

Syntax

```
no access-group acl_name
```

Parameter

acl_name
Specifies the name of a hardware ACL.

Mode

Port Interface mode

Description

Use this command to remove the assignment of a hardware ACL from the switch port.

Confirmation Command

“SHOW INTERFACE ACCESS-GROUP” on page 475

Example

This example removes the assignment of the hardware ACL “acl_10” from ports1.0.15 through 1.0.20:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.15-port1.0.20
awplus(config-if)# no access-group acl_10
```

NO ACCESS-LIST HARDWARE

Syntax

```
no access-list hardware listname
```

Parameter

listname
: Specifies the name of a hardware ACL. The name is case-sensitive.

Mode

Global Configuration mode

Confirmation Command

"SHOW ACCESS-LIST" on page 474

Description

Use this command to delete an ACL.

Note
When a hardware ACL is assigned to a class map or applied to a port interface, you cannot delete the hardware ACL.

Example

This example deletes the hardware access list "acl_5":

```
awplus> enable
awplus# configure terminal
awplus(config)# no access-list hardware acl_5
```

NO COPY-TO-MIRROR

Syntaxes

```
no copy-to-mirror mac
src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any [vlan vid]

no copy-to-mirror ip
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any] [vlan vid]

no copy-to-mirror proto proto_no
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any] [vlan vid]

no copy-to-mirroricmp
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[icmp icmp_type] [vlan vid]

no copy-to-mirror tcp|udp
src_ip_address/mask|host src_ip_address|any [src_port_no]
dst_ip_address/mask|host dst_ip_address|any [dst_port_no]
[vlan vid]
```

Parameters

src_mac_address

Specifies a source MAC address.This is the hexadecimal format:

HH:HH:HH:HH:HH:HH

dst_mac_address

Specifies a destination MAC address.The format is the same as the source MAC address.

wildcard_mask

Specifies a wildcard mask for the MAC address. This is the hexadecimal format:

XX:XX:XX:XX:XX:XX

The “X” variable can be “0” or “F.”

vid
: Specifies the VLAN ID of a receiving packet. Enter a value between 1 and 4094.

src_ip_address
: Specifies a source IPv4 address.

dst_ip_address
: Specifies a destination IPv4 address.

mask
: Specifies the mask of the IPv4 address.

proto_no
: Specifies the value of a protocol field in a packet. The range is 1 to 255.

icmp_type
: Specifies an ICMP message type. The range is 0, 3 to 5, and 8 to 18.

src_port_no
: Specifies source TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the following formulas:

  – eq *src_port_no*: Matches a packets whose port number is equal to the specified port number.

  – lt *src_port_no*: Matches packets whose port number is less than the specified port number.

  – gt *src_port_no*: Matches packets whose port number is greater than the specified port number.

  – ne *src_port_no*: Matches a packet whose port number is not equal to the specified port number.

  – range *src_port_no src_port_no*: Matches packets whose port number is within the range.

dst_port_no
: Specifies destination TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the formulas listed for the *src_port_no* parameter.

Mode

Hardware Access List mode

Confirmation Command

“SHOW ACCESS-LIST” on page 474

Description

Use this command to delete a copy-to-mirror statement from the hardware access control list. To view the list of hardware ACLs and statements configured on the switch, see “SHOW ACCESS-LIST” on page 474.

To delete a permit or deny statement, see “NO PERMIT” on page 466 or “DENY” on page 453.

Example

This example displays a list of hardware ACLs on the switch and deletes one of the copy-to-mirror statements from the hardware ACL “acl_1”:

```
awplus> enable
awplus# show access-list
Hardware IP access list acl_1
  10 deny ip any 192.168.1.0/24 vlan 10
  20 copy-to-mirror icmp 192.168.20.0/24 192.168.10.1/32
  30 copy-to-mirror mac ec:cd:6d:00:00:00 00:00:00:ff:ff:ff
any
  40 permit ip any any

awplus# configure terminal
awplus(config)# access-list hardware acl_1
awplus(config-ip-hw-acl)# no copy-to-mirror mac
ec:cd:6d:00:00:00 00:00:00:ff:ff:ff any
```

NO DENY

Syntaxes

no deny mac *src_mac_address wildcar_mask*|any
dst_mac_address wildcard_mask|any [vlan *vid*]

no deny ip *src_ip_address/mask*|host *src_ip_address*|any
dst_ip_address/mask|host *dst_ip_address*|any
[mac *src_mac_address wildcard_mask*|any
dst_mac_address wildcard_mask|any] [vlan *vid*]

no deny proto *proto_no*
src_ip_address/mask|host *src_ip_address*|any
dst_ip_address/mask|host *dst_ip_address*|any
[mac *src_mac_address wildcard_mask*|any
dst_mac_address wildcard_mask|any] [vlan *vid*]

no deny icmp *src_ip_address/mask*|host *src_ip_address*|any
dst_ip_address/mask|host *dst_ip_address*|any
[icmp *icmp_type*] [vlan *vid*]

no deny tcp|udp *src_ip_address/mask*|host *src_ip_address*|any
[*src_port_no*] *dst_ip_address/mask*|host *dst_ip_address*|any
[*dst_port_*no] [vlan *vid*]

Parameters

src_mac_address
: Specifies a source MAC address.The format is in hexadecimal in this format:

  HH:HH:HH:HH:HH:HH

dst_mac_address
: Specifies a destination MAC address.The format is the same as the source MAC address.

wildcard_mask
: Specifies a wildcard mask for the MAC address. The format is in hexadecimal in this format:

  XX:XX:XX:XX:XX:XX

  The "X" variable can be "0" or "F."

vid
: Specifies the VLAN ID of a receiving packet.

src_ip_address
: Specifies a source IPv4 address.

dst_ip_address
Specifies a destination IPv4 address.

mask
Specifies the mask of the IPv4 address.

proto_no
Specifies the value of a protocol field in a packet. The range is 1 to 255.

icmp_type
Specifies an ICMP message type. The range is 0, 3 to 5, and 8 to 18.

src_port_no
Specifies source TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the following formulas:

- eq *src_port_no*: Matches a packets whose port number is equal to the specified port number.
- lt *src_port_no*: Matches packets whose port number is less than the specified port number.
- gt *src_port_no*: Matches packets whose port number is greater than the specified port number.
- ne *src_port_no*: Matches a packet whose port number is not equal to the specified port number.
- range *src_port_no src_port_no*: Matches packets whose port number is within the range.

dst_port_no
Specifies destination TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the formulas listed for the *src_port_no* parameter.

Mode

Hardware Access List mode

Confirmation Command

“SHOW ACCESS-LIST” on page 474

Description

Use this command to delete a deny statement from the hardware access control list. To view the list of hardware ACLs and statements that are configured on the switch, see "SHOW ACCESS-LIST" on page 474.

To delete a permit or copy-to-mirror statement, see "NO PERMIT" on page 466 or "NO COPY-TO-MIRROR" on page 460.

Example

This example displays the hardware access control list on the switch and deletes a deny statement from the hardware access list "acl_2." This statement is to discard IP packets that have destination IP addresses of 192.168.1.0./24 and belong to VLAN 10:

```
awplus> enable
awplus# show access-list
Hardware IP access list acl_2
  10 deny ip any 192.168.1.0/24 vlan 10
  20 permit ip any any

awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_2
awplus(config-ip-hw-acl)# no deny ip any 192.168.1.0/24 vlan
10
```

NO PERMIT

Syntaxes

```
no permit mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any [vlan vid]

no permit ip src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any] [vlan vid]

no permit proto proto_no
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any] [vlan vid]

no permit icmp src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[icmp icmp_type] [vlan vid]

no permit tcp|udp
src_ip_address/mask|host src_ip_address|any [src_port_no]
dst_ip_address/mask|host dst_ip_address|any [dst_port_no]
[vlan vid]
```

Parameters

src_mac_address

Specifies a source MAC address. The format is in hexadecimal in this format:

HH:HH:HH:HH:HH:HH

dst_mac_address

Specifies a destination MAC address. The format is the same as the source MAC address.

wildcard_mask

Specifies a wildcard mask for the MAC address. The format is in hexadecimal in this format:

XX:XX:XX:XX:XX:XX

The “X” variable can be “0” or “F.”

vid

Specifies the VLAN ID of a receiving packet.

src_ip_address
Specifies a source IPv4 address.

dst_ip_address
Specifies a destination IPv4 address.

mask
Specifies the mask of the IPv4 address.

proto_no
Specifies the value of a protocol field in a packet. The range is 1 to 255.

icmp_type
Specifies an ICMP message type. The range is 0, 3 to 5, and 8 to 18.

src_port_no
Specifies source TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the following formulas:

- eq *src_port_no*: Matches a packets whose port number is equal to the specified port number.
- lt *src_port_no*: Matches packets whose port number is less than the specified port number.
- gt *src_port_no*: Matches packets whose port number is greater than the specified port number.
- ne *src_port_no*: Matches a packet whose port number is not equal to the specified port number.
- range *src_port_no src_port_no*: Matches packets whose port number is within the range.

dst_port_no
Specifies destination TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the formulas listed for the *src_port_no* parameter.

Mode

Hardware Access List mode

Confirmation Command

"SHOW ACCESS-LIST" on page 474

Description

Use this command to delete a permit statement from the hardware ACL. To view a list of hardware ACLs and statements that are configured on the switch, see “SHOW ACCESS-LIST” on page 474.

To delete a deny or copy-to-mirror statement, see “DENY” on page 453 or “NO COPY-TO-MIRROR” on page 460.

Example

This example displays a list of the hardware ACL and deletes a permit statement from the hardware ACL “acl_4”:

```
awplus> enable
awplus# show access-list
Hardware IP access list acl_4
  10 permit ip any 10.10.1.253
  20 permit ip 192.168.10.1/28 any
  30 deny ip any any

awplus# configure terminal
awplus(config)# access-list hardware acl_4
awplus(config-ip-hw-acl)# no permit ip 192.168.10.1/28 any
```

PERMIT

Syntaxes

```
[sequence_no] permit mac
src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any [vlan vid]

[sequence_no] permit ip
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any] [vlan vid]

[sequence_no] permit proto proto_no
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[mac src_mac_address wildcard_mask|any
dst_mac_address wildcard_mask|any] [vlan vid]

[sequence_no] permit icmp
src_ip_address/mask|host src_ip_address|any
dst_ip_address/mask|host dst_ip_address|any
[icmp icmp_type] [vlan vid]

[sequence_no] permit tcp|udp
src_ip_address/mask|host src_ip_address|any [src_port_no]
dst_ip_address/mask|host dst_ip_address|any [dst_port_no]
[vlan vid]
```

Parameters

sequence_no

Specifies a sequence number. The sequence number determines the place of the entry in the access list. When an existing sequence number is specified, the command replaces the existing entry with the new definition. If a sequence number is not specified, the command adds the entry at the end of the access list. The range of the sequence numbers is 1 to 65,535.

src_mac_address

Specifies a source MAC address that the switch filters packets based on. This is the hexadecimal format:

HH:HH:HH:HH:HH:HH

dst_mac_address

Specifies a destination MAC address that the switch filters packets on. The format is the same as the source MAC address.

wildcard_mask

Specifies a wildcard mask for the MAC address. The wildcard mask determines how much of a MAC address to apply to the MAC address match. This is the hexadecimal format:

XX:XX:XX:XX:XX:XX

The “X” variable can be “0” or “F.” Use the wildcard mask value “0” for parts of the MAC address that the switch uses to filter on. Use the wildcard mask value “F” for parts of the MAC address that the switch ignores. Specify a wildcard mask of 00:00:00:00:00:00 when you want the switch match the exact MAC address that you specify.

any

Specifies that any MAC addresses or IP addresses are used for filtering.

vid

Specifies the VLAN ID of a receiving packet that the switch filters on.

src_ip_address

Specifies a source IPv4 address that the switch filters packets on.

dst_ip_address

Specifies a destination IPv4 address that the switch filters packets on.

mask

Specifies a mask that determines how many bits of an IP address to apply to the IP address match.

host

Specifies the host keyword and an IPv4 address when you want the switch match the exact IPv4 address that you specify. The host keyword and an IPv4 address is equivalent to an IPv4 address with a mask of 32.

proto_no

Specifies the value of a protocol field in a packet that the switch filters on.The range is 1 to 255.

icmp_type

Specifies an ICMP message type. If you do not specify an ICMP message type, the switch does not filter packets on an ICMP message type. The options are:

0: Echo Reply

3: Destination Unreachable

4: Source Quench

5: Redirect

8: Echo Request

9: Router Advertisement

10: Router Solicitation

11: Time Exceeded

12: Parameter Problem

13: Timestamp

14: Timestamp Reply

15: Information Request

16: Information Reply

17: Address Mask Request

18: Address Mask Replay

src_port_no

Specifies source TCP or UDP port numbers. The range is 0 to 65,535. To specify port numbers, use one of the following five formulas:

– eq *src_port_no*: Matches packets whose port number equal to the specified port number.

– lt *src_port_no*: Matches packets whose port number is less than the specified port number.

– gt *src_port_no*: Matches packets whose port number is greater than the specified port number.

– ne *src_port_no*: Matches packets whose port number is not equal to the specified port number.

– range *src_port_no src_port_no*: Matches packets whose port number is within the range.

dst_port_no

Specifies destination TCP or UDP port numbers. The range is 0 to 65535. To specify port numbers, use one of the formulas listed for the *src_port_no* parameter.

Mode

Hardware Access List mode

Confirmation Command

“SHOW ACCESS-LIST” on page 474

Description

Use this command to add a permit statement to the hardware ACL or modify an existing permit statement. When a packet matches a permit statement, the switch forwards the packet. You can add up to 256 statements to one hardware ACL.

The hardware ACL is a sequential collection of permit, deny, or copy-to-mirror statements. The switch evaluates a packet against the statement starting with the smallest to the largest sequence number. When a packet matches the statement, the switch permits, denies, or mirrors the packet and skips the rest of the statements. If a packet does not match any statements, the switch forwards the packet.

To add or modify a deny or copy-to-mirror statement, see “DENY” on page 453 or “COPY-TO-MIRROR” on page 448.

Examples

This example creates a new hardware access list named “acl_1” and adds statements to forwards packets when the prefix of a source MAC address in the packets is “ec:cd:6d” and discard packets that do not match the source MAC address:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_1
awplus(config-ip-hw-acl)# permit mac ec:cd:6d:00:00:00
00:00:00:ff:ff:ff any
awplus(config-ip-hw-acl)# deny mac any any
```

This example creates a new hardware access list named “acl_2” and adds a statement to forward IP packets that have the destination IP address of 192.168.1.0/24 and belong to VLAN 10:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_2
awplus(config-ip-hw-acl)# permit ip any 192.168.1.0/24 vlan
10
```

This example creates a new hardware access list named "acl_3" and adds a statement to forward packets that have a protocol type of TCP, a source IP address of 192.168.10.5, and a TCP port number of 80:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware acl_3
awplus(config-ip-hw-acl)# permit tcp host 192.168.10.5 any
eq 80
```

This example adds a new statement to an existing hardware access list named "acl_4." Assume that "acl_4" consists of two statements: sequence numbers 10 and 20. To view an existing hardware access list, use SHOW ACCESS-LIST. (See "SHOW ACCESS-LIST" on page 474.) This example inserts a new permit statement with a sequence number of 15 between existing two statements:

```
awplus> enable
awplus# show access-list
Hardware IP access list acl_4
  10 permit ip 192.168.10.1/28 any
  20 deny ip any any

awplus# configure terminal
awplus(config)# access-list hardware acl_4
awplus(config-ip-hw-acl)# 15 permit ip 192.168.10.16/29 any
```

SHOW ACCESS-LIST

Syntax

```
show access-list
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the configuration of the hardware ACLs on the switch. See Figure 72 for an example.

To display the port assignments of the ACLs, see “SHOW INTERFACE ACCESS-GROUP” on page 475.

```
Hardware IP access list acl_5
    10 permit ip 192.168.10.1/28 any
    20 permit ip 192.168.10.16/29 any
    30 deny ip any any
```

Figure 72. SHOW ACCESS-LIST Command

Examples

This example displays the configuration of the hardware ACL named “acl_5”:

```
awplus# show access-list acl_5
```

This example displays all the hardware ACLs on the switch:

```
awplus# show access-list
```

SHOW INTERFACE ACCESS-GROUP

Syntax

```
show interface port_ids access-group acl_name
```

Parameters

port_ids
Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

acl_name
Specifies the name of a hardware ACL.

Mode

Privileged Exec mode

Description

Use this command to display the port assignments of the hardware ACLs. See Figure 73 for an example of the command output.

```
Interface port1.0.1
   access-group acl_10
Interface port1.0.2
   access-group acl_10
```

Figure 73. SHOW INTERFACE ACCESS-GROUP Command

Example

This example displays a hardware ACL for ports 1.0.1 and 1.0.2:

```
awplus# show interface port1.0.1,port1.0.2 access-group
```

SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION

Syntax

```
show platform classifier statistics utilization
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the consumption of the memory on the switching chip that is allocated to DoS, ACL, and Quality of Service (QoS) functions. An example of the command output is shown in Figure 74.

```
Number of Entries:
Policy Type  Unit    Group ID   Used / Total
-------------------------------------------------
DoS          0       1          104  / 256 (40%)
ACL          0       2            4  / 256  (1%)
QoS          0       3          255  / 256 (99%)
```

Figure 74. SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION Command

Note
This command is equivalent to the SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION BRIEF command.

The fields are described in Table 75.

Table 75. SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION Command Description

Field	Description
Policy Type	Displays a policy type. The options are: ❒ DoS ❒ ACL ❒ QoS

Table 75. SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION Command Description (Continued)

Field	Description
Unit	Indicates the ID of the switching chip. It always displays "0" for this switch.
Group ID	DIsplays the group ID.
Used	Displays the number of units of memory consumed by the policy type.
Total	Displays the total number of memory units allocated to the policy type. It is always 256 units on this switch.

Figure 75. SHOW PROGRESS Command

Example

This example displays the memory consumption configuration of the switch per policy type:

```
awplus# show platform classifier statistics utilization
```

Chapter 21
Quality of Service (QoS) Commands

The Quality of Service (QoS) commands are summarized in Table 76 and described in detail in this chapter.

Table 76. Quality of Service Commands

Command	Mode	Description
“CLASS” on page 481	Policy Map Configuration	Associates an existing class map to a policy map.
“CLASS-MAP” on page 483	Global Configuration	Creates a class map and enters the Class Map Configuration mode.
“DEFAULT-ACTION” on page 485	Policy map Configuration	Sets the action for the default class-map belonging to the specified policy map.
“DESCRIPTION (Policy Map)” on page 487	Policy Map Configuration	Adds a description of the policy map.
“MATCH ACCESS-GROUP” on page 489	Class Map Configuration	Adds a hardware ACL to a class map.
“MATCH COS” on page 491	Class Map Configuration	Sets the value of the Class of Service (CoS) for a class-map.
“MATCH DSCP” on page 492	Class Map Configuration	Sets the value of DSCP to a class map.
“MATCH ETH-FORMAT PROTOCOL” on page 493	Class Map Configuration	Adds an Ethernet frame format and Layer 3 protocol as matching criteria to a class map.
“MATCH IP-PRECEDENCE” on page 496	Class Map Configuration	Sets the value of IP precedence to a class map.
“MATCH MAC-TYPE” on page 497	Class Map Configuration	Sets the MAC address type to a class map.
“MATCH TCP-FLAGS” on page 499	Class Map Configuration	Sets one or more TCP flags for a class map.
“MATCH VLAN” on page 501	Class Map Configuration	Sets a VLAN ID for a class map.

Table 76. Quality of Service Commands (Continued)

Command	Mode	Description
“MLS QOS COS” on page 502	Port Interface	Assigns a Class of Service (CoS) value to untagged frames that enter the specified port.
“MLS QOS ENABLE” on page 503	Global Configuration	Enables QoS on the switch.
“MLS QOS MAP COS-QUEUE” on page 504	Interface Configuration	Maps CoS values to port egress queues.
“NO MATCH ACCESS-GROUP” on page 506	Class Map Configuration	Removes a hardware ACL as a matching criterion from a class map.
“NO MLS QOS ENABLE” on page 507	Global Configuration	Disables QoS and deletes all the QoS settings on the switch.
“POLICY-MAP” on page 508	Global Configuration	Creates a policy map and enters the Policy Map Configuration mode.
“PRIORITY-QUEUE” on page 510	Port Interface	Specified egress queues to use the Strict Priority Queue (PQ) method to schedule queues.
“SERVICE-POLICY INPUT” on page 511	Interface Configuration	Associates a policy map with a port interface.
“SHOW CLASS-MAP” on page 513	Privileged Exec	Displays the settings of a class map.
“SHOW POLICY-MAP” on page 515	Privileged Exec	Displays the settings of a policy map.
“SHOW MLS QOS” on page 518	Privileged Exec	Displays the status of QoS.
“SHOW MLS QOS INTERFACE” on page 519	Privileged Exec	Displays the QoS settings of the specified ports.
“SHOW MLS QOS MAPS COS-QUEUE” on page 521	Privileged Exec	Displays the mappings of CoS values to egress queues.
“WRR-QUEUE EGRESS-RATE-LIMIT QUEUES” on page 522	Port Interface	Sets a limit on the amount of traffic that can be transmitted from the specified queues.
“WRR-QUEUE WEIGHT” on page 524	Port Interface	Configures Weighted Round-Robin (WRR) based scheduling on the specified ports.

CLASS

Syntax

`class` *`class_name`*`|default`

Parameters

`class_name`
Specifies the name of a class map.

`default`
Specifies the default class map.

Mode

Policy Map Configuration mode

Description

Use this command to associate an existing class map to a policy map. When a policy map is applied to a port, the switch applies criteria defined in the class maps associated with the policy map to incoming traffic on the port. The switch checks traffic in the order in which the class maps are added to the policy map. You can associate up to 256 class maps with a policy map.

This command enters the Policy Map Class Configuration mode; however, no commands are available in this mode.

When you create a policy map, a default class map is added to it automatically. The default class map is applied to traffic after all the user-defined class maps are checked. To change the action of the default class map, use the DEFAULT ACTION command. See "DEFAULT-ACTION" on page 485.

Entering the CLASS command with the default keyword does not affect the policy map. In addition, you cannot delete the default class map.

To remove a class map from a policy map, use the NO CLASS command with the class_name parameter specified.

Confirmation Commands

"SHOW POLICY-MAP" on page 515

Examples

This example creates a policy map called “pmap1,” then associates a class map called “cmap5” to policy map “pmap1”:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap5
awplus(config-pmap-c)#
```

This example deletes an association between a class-map called “cmap5” and policy map called “pmap1”:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no class cmap5
```

CLASS-MAP

Syntax

```
class-map class_name
```

Parameter

class_name

Specifies the name of a class map. The name is case-sensitive and can be up to 63 alphanumeric characters. Special characters except spaces, exclamation marks (!), and question marks are allowed. The name "default" is reserved for the default class map and cannot be used.

Mode

Global Configuration mode

Description

Use this command to create a class map and access the Class Map Configuration mode. You can create up to 256 class maps on the switch.

A class map consists of:

- one or more matching criteria
- one action

When a class map includes multiple matching criteria, the switch filters incoming traffic with an AND operand. Incoming traffic must meet all the matching criteria in a class map to be taken an action.

The action of a class map can be permit, deny, or copy-to-mirror. By default, the action of a class map is permit. When a class map includes a hardware ACL, the action of the class map is the action defined in the hardware ACL.

To apply a class map to take an action for classified traffic, you must assign one or more class maps to a policy map.Then assign the policy map to a port. To assign a class map to a policy map, see "CLASS" on page 481.

You can also modify an existing class map with this command; however, you cannot modify or delete a class map when the class map is assigned to a policy map. Use NO CLASS command with the class_name parameter specified to remove a class map from the associated policy map.

You must enable QoS on the switch to use this command. To enable QoS, see “MLS QOS ENABLE” on page 503.

To delete a class map, use the NO CLASS-MAP command.

Confirmation Command

“SHOW CLASS-MAP” on page 513

Examples

To create a class-map called “cmap1” and access the Configuration Class-map mode, do the following:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)#
```

To delete a class-map called “cmap1,” do the following:

```
awplus> enable
awplus# configure terminal
awplus(config)# no class-map cmap1
```

DEFAULT-ACTION

Syntax

```
default-action permit|deny|copy-to-mirror
```

Parameters

permit
: Specifies packets are permitted. This is the default setting.

deny
: Specifies packets are denied.

copy-to-mirror
: Specifies packets to be copied and sent to the mirror port. The mirror port must be defined using the MIRROR command. See "MIRROR" on page 247.

Mode

Policy Map Configuration mode

Description

Use this command to change the action of the default class map belonging to a particular policy map. A policy map consists of one default class map as well as user-defined class maps.

The action of the default class map is applied to any packet that does not meet the criteria specified by the class maps in the policy map.

To restore the default setting of the permit action, use NO DEFAULT-ACTION command.

Confirmation Command

"SHOW POLICY-MAP" on page 515

Examples

This example sets the action for the default class-map to deny:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)#default-action deny
```

This example resets the action for the default class-map to permit:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no default-action
```

DESCRIPTION (Policy Map)

Syntax

```
description line
```

Parameter

line

Specifies a description of the policy map. The line can be up to 80 alphanumeric characters. Spaces and special characters are allowed with the exception of the exclamation mark (!) and question mark (?).

Mode

Policy Map Configuration mode

Description

Use this command to add a description to the specified policy map.

To delete a description from the policy map, use the NO DESCRIPTION command.

Confirmation Command

"SHOW POLICY-MAP" on page 515

Examples

This example adds a description of "VOIP traffic" to a policy map called "pmap20":

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap20
awplus(config-pmap)# description VOIP traffic
```

This example adds a description of "Video traffic" to a policy map called "pmap1":

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# description Video traffic
```

To remove a description from a policy map called “pmap1,” do the following:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no description
```

MATCH ACCESS-GROUP

Syntax

```
match access-group acl_name
```

Parameter

acl_name
Specifies the name of a hardware ACL.

Mode

Class Map Configuration mode

Description

Use this command to add a hardware ACL as matching criteria to a class map. When a hardware ACL has already been added to a class map, this command replaces the previous value with the new value.

Confirmation Command

"SHOW CLASS-MAP" on page 513

Examples

This example creates a hardware ACL named "aclssh," which permits SSH traffic only from IP addresses 10.100.10.70 to 10.100.10.100 and denies SSH traffic from the other source addresses. Then, the example creates a class map named "ssh," and adds the "aclssh" hardware ACL to the "ssh" class map:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware aclssh
awplus(config-ip-hw-acl)# permit tcp 10.100.10.7/32
10.100.10.100/32 eq 22
awplus(config-ip-hw-acl)# deny tcp any any eq 22
awplus(config-ip-hw-acl)# exit
awplus(config)# class-map ssh
awplus(config-cmap)# match access-group aclssh
```

This example creates a hardware ACL named “aclping” to block IP addresses 192.168.0.0 to 192.168.255.255 from pinging and adds the “aclping” hardware ACL to the class map “denyPingFrom192”:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list hardware aclping
awplus(config-ip-hw-acl)# deny icmp 192.168.0.0./16 any
icmp-type 8
awplus(config-ip-acl)# exit
awplus(config)# class-map denyPingFrom192
awplus(config-cmap)# match access-group aclping
```

MATCH COS

Syntax

```
match cos value
```

Parameter

value
Specifies the CoS value. The range is 0 to 7.

Mode

Class Map Configuration mode

Description

Use this command to add a CoS value as a matching criterion to a class map. When a CoS value has already been added to a class map, this command replaces the previous value with the new value.

When a CoS value is assigned, the switch compares the specified CoS value against the CoS value in the tagged VLAN field in frames. CoS values in untagged frames are assigned at receiving ports specified by "MLS QOS COS" on page 502.

To remove the CoS value as a matching criterion from a class map, use the NO MATCH COS command.

Confirmation Commands

"SHOW CLASS-MAP" on page 513

Examples

This example creates a class map, called "cmap1," and adds a CoS value of 4 as a matching criteria to the class map:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match cos 4
```

This example removes the CoS matching value from the "cmap1" class map:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match cos
```

MATCH DSCP

Syntax

```
match dscp value
```

Parameter

value
Specifies the DSCP value. The range is 0 to 63.

Mode

Class Map Configuration mode

Description

Use this command to add a DiffServ Code Point (DSCP) value as a matching criterion to a class map. When a DSCP value has already been specified to a class map, this command replaces the previous value with the new value.

When a DSCP value is assigned, the switch compares the specified DSCP value against the value of the DSCP field in the IP header.

To remove the DSCP value as a matching criterion from a class map, use the NO MATCH DSCP command.

Confirmation Command

“SHOW CLASS-MAP” on page 513

Examples

The following example creates a class map, called “cmap1,” that matches ingress traffic with a DSCP value of 56:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match dscp 56
```

The following example removes the DSCP value from class map “cmap1”:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match dscp
```

MATCH ETH-FORMAT PROTOCOL

Syntax

```
match eth-format format protocol type
```

Parameters

format

Specifies the Ethernet frame format. The options are listed in Table 77.

Table 77. MATCH ETH-FORMAT PROTOCOL Command FORMAT KEYWORDS

Keyword	Description
ethii-any	Ethernet Version 2 with tagged or untagged VLAN
ethii-untagged	Ethernet Version 2 with untagged VLAN
ethii-tagged	Ethernet Version 2 with tagged VLAN
802dot2-untagged	802.2 LLC with untagged VLAN
802dot2-tagged	802.2 LLC with tagged VLAN
netwareraw-untagged	Novell 802.3 raw with untagged VLAN
netwareraw-tagged	Novell 802.3 raw with tagged VLAN
snap-untagged	802.2 LLC + SNAP with untagged VLAN
snap-tagged	802.2 LLC + SNAP with tagged VLAN

type

Specifies the number of the Layer 3 protocol in hexadecimal. You can also specify a pre-defined keyword. The pre-defined keywords are listed in Table 78 on page 494.

Table 78. MATCH ETH-FORMAT PROTOCOL Command TYPE KEYWORDS

Keyword	Protocol No. (hexadecimal)	Keyword	Protocol No. (hexadecimal)
any	N/A	ethertalk-2-aarp	80F3
appletalk	809B	ibm-sna	80D5
appletalk-aarp	80F3	ip	0800
arp	0806	ipv6	86DD
banyan-systems	0BAD	ipx	8137
bbn-simnet	5208	ipx-802dot2	E0
chaosnet	0804	ipx-802dot3	FFFF
dec-customer	6006	ipx-snap	8137
dec-decnet	6003	iso-clns-is	FE
dec-diagnostic	6005	nbs-internet	0802
dec-encryption	803D	netbeui	F0
dec-langridge	8038	proway	8E
dec-lat	6004	proway-lan	0E
dec-lavc	6007	rarp	8035
dec-mop-dump-ld	6001	sna-path-control	04
dec-mop-rem-cdons	6002	snmp	814C
ecma-internet	0803	xdot25-level-3	0805
eia-rs	4E	xdot72-internet	0801
ethertalk-2	809B	xns-compat	0807

Mode

Class Map Configuration mode

Description

Use this command to add an Ethernet frame format and Layer 3 protocol as matching criteria to a class map. You must specify a Layer 3 protocol for the specified Ethernet frame format. The switch matches the specified Ethernet frame format to the value of the Ether type field in incoming frames and the specified Layer 3 protocol to the value of the protocol field

in the packet. When an Ethernet frame format and Layer 3 protocol have already been set in a class map, this command replaces the previous value with the new one.

You can specify the ANY keyword as the Layer 3 protocol only when you specify the Ethernet frame format as either NETWARERAW-UNTAGGED or NETWARERAW-TAGGED.

To specify frames, including the VLAN tag field, as a matching criterion, specify the ETHII-TAGGED keyword and a protocol. You cannot specify 8100 as a protocol number.

To remove an Ethernet frame format and Layer 3 protocol as matching criteria from a class map, use the NO MATCH ETH-FORMAT PROTOCOL command.

Confirmation Command

"SHOW CLASS-MAP" on page 513

Example

The following example specifies Ethernet Version 2 with the tag field as the Ethernet frame format and ARP as the protocol to the "cmap7" class map:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap7
awplus(config-cmap)# match eth-format ethii-tagged protocol
0806
```

MATCH IP-PRECEDENCE

Syntax

```
match ip-precedence value
```

Parameter

value
: Specifies the value of the Type of Service (TOS) priority (IP precedence) field in the IP header. The range is 0 to 7.

Mode

Class Map Configuration mode

Description

Use this command to add a precedence value as a matching criterion to a class map. When a precedence value has already been added to a class map, this command replaces the previous value with the new value.

When a precedence value is assigned, the switch compares the specified precedence value against the value of the TOS priority field in the IP header.

To remove the precedence value as a matching criterion from a class map, use the NO MATCH IP-PRECEDENCE command.

Confirmation Commands

“SHOW CLASS-MAP” on page 513

Examples

The following example creates a class map called, “cmap7,” to evaluate all ingress IPv4 packets for a precedence value of 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap7
awplus(config-cmap)# match ip-precedence 5
```

The following example removes the IP precedence value from class map “cmap7”:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap4
awplus(config-cmap)# no match ip-precedence
```

MATCH MAC-TYPE

Syntax

```
match mac-type l2bcast|l2mcast|l2ucast
```

Parameters

`l2bcast`
Specifies the Layer 2 Broadcast frames as the destination MAC address type.

`l2mcast`
Specifies the Layer 2 Multicast frames as the destination MAC address type.

`l2ucast`
Specifies the Layer 2 Unicast frames as the destination MAC address type.

Note
All three keywords l2bcast, l2mcast, and l2uncast, start with the letter "l" and the number "2" to represent Layer 2.

Mode

Class Map Configuration mode

Description

Use this command to add the type of destination MAC address as a matching criterion to a class map. When the MAC address type has already been assigned to a class map, this command replaces the previous value with the new value.

When the MAC address type is assigned, the switch compares the MAC address type against the Layer 2 address type of incoming frames.

To remove the MAC address type as a matching criterion from a class map, use the NO MATCH MAC-TYPE command.

Confirmation Command

"SHOW CLASS-MAP" on page 513

Examples

This example sets the class-map's MAC address type to Layer 2 broadcast frames:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match mac-type l2bcast
```

The following example removes the MAC type from a class map:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match mac-type
```

MATCH TCP-FLAGS

Syntax

```
match tcp-flags acl|syn|fin|rst|urg
```

Parameters

`acl`
Specifies the ACK (acknowledge) TCP flag.

`syn`
Specifies the SYN (synchronize) TCP flag.

`fin`
Specifies the FIN (finish) TCP flag.

`rst`
Specifies the RST (reset) TCP flag.

`urg`
Specifies the URG (urgent) TCP flag.

Mode

Class Map Configuration mode

Description

Use this command to add one or multiple TCP flags as matching criteria to a class map. A TCP flag is a control bit set in a TCP header. If a packet contains a TCP header, the switch matches the criteria to the FLAGS field in the TCP header. When a TCP flag has already been set in a class map, this command adds a new flag as matching criterion.

When multiple TCP flags are specified as matching criteria to a class map, the switch filters incoming traffic with an AND operand.

To remove a TCP flag as a matching criterion from a class map, use the NO MATCH TCP-FLAGS command.

Confirmation Command

"SHOW CLASS-MAP" on page 513

Examples

This example adds the SYN and ACK flags as matching criteria to the class map called “tcpstart”:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map tcpstart
awplus(config-cmap)# match tcp-flags syn ack
```

This example removes the ACK flag as a matching criterion from the class map “tcpstart”:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map tcpstart
awplus(config-cmap)# no match tcp-flags ack
```

MATCH VLAN

Syntax

```
match vlan vid
```

Parameter

vid
Specifies the VLAN ID number. The range is 1 to 4094.

Mode

Class Map Configuration mode

Description

Use this command to add the VLAN ID as a matching criterion to a class map. When the VLAN ID has already been specified to a class map, this command replaces the previous value with the new value.

When the VLAN ID is assigned, the switch compares the specified VID against the VID in the tagged VLAN field (in packets) or the VID of either the MAC address VLAN or a port VLAN with untagged VLAN packets.

To remove the VLAN ID as a matching criterion from a class map, use the NO MATCH VLAN command.

Confirmation Command

"SHOW CLASS-MAP" on page 513

Examples

This example creates a class map called "cmap3" and adds VLAN 5 as a matching criterion:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap3
awplus(config-cmap)# match vlan 5
```

This example removes VLAN ID as a matching criterion from the class map "cmap3":

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map cmap3
awplus(config-cmap)# no match vlan
```

MLS QOS COS

Syntax

```
mls qos cos cos_value
```

Parameter

cos_value
: Specifies the Class of Service (CoS) value. The range is 0 to 7. The default value is 0.

Mode

Port Interface mode

Description

Use this command to assign a CoS value to untagged frames that enter the specified port. By default, CoS values in all untagged frames are assigned a value of 0.

You must enable QoS on the switch to use this command. To enable QoS, see “MLS QOS ENABLE” on page 503.

To restore the default CoS value of 0 for untagged frames, use the NO MLS QOS COS command.

Confirmation Command

“SHOW MLS QOS INTERFACE” on page 519

Examples

The following example sets the CoS value to 1 on ports 1.0.1 to 1.0.24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1-1.0.24
awplus(config-if)# mls qos cos 1
```

The following example sets the CoS priority value to 4 on port 1.0.22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22
awplus(config-if)# mls qos cos 4
```

MLS QOS ENABLE

Syntax

```
mls qos enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to enable the QoS feature on the switch. By default, the QoS feature is disabled.

Confirmation Command

"SHOW MLS QOS" on page 518

Example

This example enables the QoS feature on the switch:

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

MLS QOS MAP COS-QUEUE

Syntax

`mls qos map cos-queue` *`cos_value`* `to` *`queue`*

Parameters

`cos_value`
Specifies the Class of Service (CoS) value. The range is 0 to 7. The default value is 0.

`queue`
Specifies an egress queue number. The range is 0 to 7, where 7 is the highest priority queue.

Mode

Interface Configuration mode

Description

Use this command to map CoS values to egress queues. The switch forwards packets in the queue with the highest priority value. The switch refers to the CoS-queue map when assigning packets to egress queues after packets are assigned to egress ports.

Table 79 shows the default mappings between the CoS and egress queues.

Table 79. CoS Queue MAP: Default Setting

CoS	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

You must enable QoS on the switch to use this command. To enable QoS, see “MLS QOS ENABLE” on page 503.

To restore the default mappings between the CoS and Queue, use the NO MLS QOS MAP COS-QUEUE command.

Confirmation Command

“SHOW MLS QOS MAPS COS-QUEUE” on page 521

Examples

This example maps the CoS value 6 to the egress queue 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# mls qos map cos-queue 6 to 7
```

This example restores the default mappings of the CoS and queue:

```
awplus> enable
awplus# configure terminal
awplus(config))# no mls qos map cos-queue
```

NO MATCH ACCESS-GROUP

Syntax

```
no match access-group acl_name
```

Parameter

acl_name
Specifies the name of a hardware ACL.

Mode

Class Map mode

Description

Use this command to remove a hardware ACL as a matching criteria from a class map.

Confirmation Command

“SHOW RUNNING-CONFIG” on page 116

Example

This example removes the hardware ACL access list “aclping” from a class map called “denyPingFrom192”:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map denyPingFrom192
awplus(config-cmap)# no match access-group aclping
```

NO MLS QOS ENABLE

Syntax

```
no mls qos enable
```

Parameters

None

Mode

Global Configuration mode

Description

Use this command to disable the QoS feature on the switch.

Caution
When QoS is disabled, the QoS settings, including policy maps and class maps, are all deleted.

Example

This example disables the QoS feature and delete all the QoS settings on the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# no mls qos enable
```

POLICY-MAP

Syntax

```
policy-map policy_name
```

Parameter

policy_name
: Specifies the name of a policy map. The policy map name is case-sensitive and can be up to 63 alphanumeric characters.

Mode

Global Configuration mode

Description

Use this command to create a policy map and enter the Policy Map Configuration mode. A policy map consists of user-defined class maps and one default class map. You can create up to 64 policy maps on the switch.

To apply a policy map to take an action on classified traffic, you must assign a group of class maps to a policy map and assign it to a port. To assign class maps to a policy map, see “CLASS” on page 481. To assign a policy map to a port, see “SERVICE-POLICY INPUT” on page 511. Within the class map, you can assign one of three actions to be performed on the traffic specified —permit, deny, or copy the traffic to the mirror port.

A policy map consists of one or more user-defined class maps and one default class map. The default class map is included in a policy map automatically and applied to the traffic after all user-defined class maps are evaluated. You can change the action of the default class map; however, the traffic that the action is applied to is always the traffic that did not match any criteria defined in the class maps. To change the action of the default class map, see “DEFAULT-ACTION” on page 485.

You can also modify an existing policy map with this command; however, you *cannot* modify or delete a policy map when the policy map is assigned to a port. Use NO SERVICE-POLICY INPUT command to remove a policy map from the associated port. See “SERVICE-POLICY INPUT” on page 511.

You must enable QoS on the switch to use this command. To enable QoS, see “MLS QOS ENABLE” on page 503.

To delete a policy map, use the NO POLICY-MAP command.

Confirmation Command

"SHOW MLS QOS INTERFACE" on page 519

Examples

This example creates a policy map called "pmap1" and enters the Policy Map Configuration mode:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)#
```

This example deletes a policy map called "pmap5":

```
awplus> enable
awplus# configure terminal
awplus(config)# no policy-map pmap5
```

PRIORITY-QUEUE

Syntax

```
priority-queue queue_numbers
```

Parameter

queue_numbers
: Specifies one or multiple numbers of egress queues to use the Strict Priority Queuing (PQ) technique. The queue number can be 0 to 7. Use a space to separate numbers. By default, all egress queues are specified in Strict PQ.

Mode

Port Interface mode

Description

Use this command to specify egress queues in the specified port to use the Strict Priority Queuing (PQ) technique to schedule queues. In Strict PQ, packets in a high-priority queue are scheduled before packets in lower-priority queues. The switch empties a queue before moving to a lower-priority queue.

Strict PQ has higher priority than WRR queuing. When a port uses both Strict PQ and Weight Round Robin (WRR) scheduling, packets in WRR queues are not forwarded until queues in Strict PQ are emptied.

You must enable QoS on the switch to use this command. To enable QoS, see “MLS QOS ENABLE” on page 503.

Confirmation Command

“SHOW MLS QOS INTERFACE” on page 519

Example

This example specifies egress queues on the port 1.0.10 to use the Strict PQ technique:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.10
awplus(config-if)# priority-queue 0 1 2 3 4 5 6 7
```

SERVICE-POLICY INPUT

Syntax

```
service-policy input policy_name
```

Parameter

policy_name
Specifies the name of a policy map to associate with a port.

Mode

Interface Configuration mode

Description

Use this command to apply a policy map to one or more ports. When a policy map is applied to a port, the switch filters incoming traffic on the port and take actions based on class maps in the policy map.

You can assign only one policy map to a port; however, you can assign the same policy map to multiple ports. For example, you can assign policy map, pmap1, to ports 1.0.1 to 1.0.5. Once you have assigned pmap1 to these ports, you cannot assign a second policy map to the same ports. It is important to note that when the memory allocated to policy maps on the switching chip runs out of space, you cannot apply any more policy maps to ports.

When DoS (Denial of Service), hardware ACLs, and policy maps, or any combinations of two features are applied to a port, incoming packets must pass all the criteria to be forwarded. The switch applies DoS, hardware ACLs, and policy maps to incoming packets in this order.

The switch does not apply policy maps to packets that the switch sends out. In addition, the switch does not apply policy maps to IGMP packets when IGMP snooping is enabled.

You must enable QoS on the switch to use this command. To enable QoS, see "MLS QOS ENABLE" on page 503.

To remove a policy map from the associated port, use the NO SERVICE-POLICY INPUT command.

Examples

The following example applies policy map “pmap1” to port 1.0.5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# service-policy input pmap1
```

The following example applies the policy map “pmap2” to port 1.0.12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.12
awplus(config-if)# service-policy input pmap2
```

The following example removes the application between policy map “pmap3” and port 1.0.17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# no service-policy input pmap3
```

SHOW CLASS-MAP

Syntax

```
show class-map name
```

Parameter

name

Specifies the name of a class map. The name is case-sensitive and can be up to 63 alphanumeric characters.

Modes

Privileged Exec

Description

Use this command to display the settings of the specified class map. When you do not specify a class name, the command displays all the class maps defined on the switch. See Figure 76 for an example of this command.

```
CLASS-MAP-NAME: cmap1
   Match IP DSCP: 10
   Match Mac Type: 12ucast

CLASS-MAP-NAME: cmap2
   Match IP DSCP: 20
   Match Mac Type: 12ucast
```

Figure 76. SHOW CLASS-MAP Command

The fields are described in Table 80.

Table 80. SHOW CLASS-MAP Command

Field	Description
CLASS-MAP-NAME	Displays the name of a class map.
QOS-ACCESS-LIST NAME	Displays the name of hardware ACL set by the MATCH ACCESS-GROUP command.
Match vlan	Displays the VID set by the MATCH VLAN command.
Match IP DSCP	Displays the value of DSCP set by the MATCH DSCP command.

Table 80. SHOW CLASS-MAP Command (Continued)

Field	Description
Match IP precedence	Displays the value of IP precedence set by the MATCH IP-PRECEDENCE command.
Match CoS	Displays the CoS value set by the MATCH CoS command.
Match TCP Flags	Displays the settings of TCP flags set by the MATCH TCP FLAGS command.
Match Mac Type	Displays the MAC address type set by the MATCH MAC-TYPE command.
Match Eth Format / Match protocol	Displays the settings set by the MATCH ETH-FORMAT PROTOCOL command.

Examples

This example displays the settings of the class map called “cmap1”:

```
awplus# show class-map cmap1
```

This example displays the settings of all the class maps defined on the switch”:

```
awplus# show class-map
```

SHOW POLICY-MAP

Syntax

```
show policy-map policy_name
```

Parameter

policy_name
: Specifies the name of a policy map. The policy map name is case-sensitive and can be up to 63 alphanumeric characters.

Modes

Privileged Exec

Description

Use this command to display a list of the policy maps configured on the switch. When you do not specify a class name, the command displays all the class maps defined on the switch. See Figure 77 for an example of this command.

```
POLICY-MAP-NAME: pmap1
   State: detached
   Default class-map action: permit

      CLASS-MAP-NAME: default

POLICY-MAP-NAME: pacl10
   State: attached
   Description: policy-based ACL 10
   Default class-map action: permit

   CLASS-MAP-NAME: default

   CLASS-MAP-NAME: permitSA10
      QOS-ACCESS-LIST-NAME: SA10
      Match TCP Flags: ack syn

   CLASS-MAP-NAME: denyS10
      QOS-ACCESS-LIST-NAME: S10
      Match TCP Flags: syn
```

Figure 77. SHOW POLICY-MAP Command

The fields are described in Table 81.

Table 81. SHOW POLICY-MAP Command Description

Field	Description
POLICY-MAP-NAME	Displays the name of the policy map set by the POLICY-MAP command.
State	Displays if the policy map is assigned to a port. The options are: ❒ attached: Indicates a policy map is assigned to a port. ❒ detached: Indicates a policy map is not assigned to a port. Port assignment is specified using the SERVICE-POLICY INPUT command.
Description	Displays the description of the policy map set with the DESCRIPTION command.
Default class-map action	Displays the action of the default class map set with the DEFAULT-ACTION command.
CLASS-MAP-NAME	Displays the name of a class map assigned to the policy map. Class map assignment is specified with the CLASS command.
Match vlan	Displays the VID set by the MATCH VLAN command.
Match IP DSCP	Displays the value of DSCP set by the MATCH DSCP command.
Match IP precedence	Displays the value of IP precedence set by the MATCH IP-PRECEDENCE command.
Match CoS	Displays the CoS value set by the MATCH CoS command.
Match TCP Flags	Displays the settings of TCP flags set by the MATCH TCP FLAGS command.
Match Mac Type	Displays the MAC address type set by the MATCH MAC-TYPE command.
Match Eth Format / Match protocol	Displays the settings set by the MATCH ETH-FORMAT PROTOCOL command.

Example

This example displays the settings of a policy map called "pmap1":

```
awplus# show policy-map pmap1
```

SHOW MLS QOS

Syntax

```
show mls qos
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the status of the QoS feature. The options are:

- Enable
- Disable

Example

This example displays the status of the QoS feature:

```
awplus# show mls qos
```

SHOW MLS QOS INTERFACE

Syntax

```
show mls qos interface port_ids
```

Parameter

port_ids
Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Mode

Privileged Exec mode

Description

Use this command to display the QoS settings of the specified ports. See Figure 78 for an example of the command output.

```
Interface: port1.0.1

   INPUT-POLICY-MAP-NAME: pacl10
     CLASS-MAP-NAME: default
     CLASS-MAP-NAME: permitSA10
        QOS-ACCESS-LIST-NAMT: SA10
        Match TCP Flags: ack syn
     CLASS-MAP-NAME: denyS10
        QOS-ACCESS-LIST-NAME: S10
        Match TCP Flags: syn

   Default CoS: 3
   Number of egress queue: 8

   Egress Queue:          0
      Status:             Enabled
      Scheduler:          Weighted Round Robin
      Weight:             1
      Queue Limit:        -
      Egress Rate Limit: 30720 kb

   Egress Queue:          1
      Status:             Enabled
      Scheduler:          Weighted Round Robin
      Weight:             1
      Queue Limit:        -
      Egress Rate Limit: 30720 kb
```

Figure 78. SHOW MLS QOS INTERFACE Command

The fields are described in Table 82.

Table 82. SHOW MLS QOS INTERFACE Command

Field	Description
Interface	Displays the port ID.
INPUT-POLICY-MAP-NAME	Displays the name of the policy map assigned to the port. Information about the policy map, such as class maps, and matching criteria are also displayed. It displays the above information only when the port is assigned to a policy map.
Default CoS	Displays the CoS value set on the port. This CoS value is assigned only to untagged frames when received at this port. The CoS value is only displayed when the value is not the default value of 0.
Number of egress queues	Displays the number of egress queues on the port. Each port on the switch has eight queues.
Egress Queue	Displays the egress queue number.
Status	Displays the status of the egress queue. The options are: ❒ Enabled ❒ Disabled
Scheduler	Displays the scheduler that the egress queue applies. The options are: ❒ Strict Priority ❒ Weighted Round-Robin
Weight	Displays the weight specified to the egress queue. This field is displayed only when the egress queue's scheduler is WRR.
Queue Limit	Not supported.
Egress Rate Limit	Displays the maximum egress rate specified on the port. When the rate is not set, this field displays 0 Kb.

Example

This example displays the QoS settings on port 1.0.3:

```
awplus# show mls qos interface port1.0.3
```

SHOW MLS QOS MAPS COS-QUEUE

Syntax

```
show mls qos maps cos-queue
```

Parameters

None

Mode

Privileged Exec mode

Description

Use this command to display the mappings of CoS values to egress queues. See Figure 79 for an example of the default mapping.

```
COS-TO-QUEUE-MAP:
   COS:      0 1 2 3 4 5 6 7
----------------------------
   QUEUE:    2 0 1 3 4 5 6 7
```

Figure 79. SHOW MLS QOS MAPS COS-QUEUE Command

Example

This example displays the mappings of CoS values to egress queues:

```
awplus# show mls qos maps cos-queue
```

WRR-QUEUE EGRESS-RATE-LIMIT QUEUES

Syntax

```
wrr-queue egress-rate-limit bandwidth queues queue_numbers
```

Parameters

bandwidth

Specifies the maximum data. The options are:

- 1k to 41943040k: The k indicates Kbps. You can omit the k. The maximum bandwidth for 10 Gigabit Ethernet ports is 10485760.
- 1m to 40960m: The m indicates Mbps. The maximum bandwidth for 10 Gigabit Ethernet ports is 10240m. You must specify the m.
- 1g to 40g: The g indicates Gbps. The maximum bandwidth for 10 Gigabit Ethernet ports is 10g. You must specify the g.

The units k, m, and g are not case-sensitive.

queue_numbers

Specifies one or multiple numbers of egress queues. The queue number can be 0 to 7. Use a space to separate numbers.

Mode

Port Interface mode

Description

Use this command to set a limit on the bandwidth of egress queues on the specified ports for the switch to perform traffic shaping. Traffic shaping is a traffic management technique used to avoid congestion by meeting downstream requirements and regulating the flow of traffic.

When the maximum bandwidth that you specify is not an increment of 8 Kbps, the system changes to a number that is larger than the specified bandwidth and the closest increment of 8 Kbps.

You must enable QoS on the switch to use this command. To enable QoS, see “MLS QOS ENABLE” on page 503.

To remove the maximum bandwidth specified on queues on the specified ports, use the NO WRR_QUEUE EGRESS-RATE-LIMIT QUEUES command.

Confirmation Command

"SHOW RUNNING-CONFIG" on page 116

Examples

This example sets the maximum bandwidth on queues 0, 1, and 2 on port 1.0.7 to 1 Gbits/second:

```
awplus> enable
awplus# configure terminal
awplus(config)# mls qos enable
awplus(config-if)# interface port1.0.7
awplus(config-if)# wrr-queue egress-rate-limit 1g queues 0 1
2
```

This example removes the maximum bandwidth set on queues 0 and 1 on port 1.0.7:

```
awplus> enable
awplus# configure terminal
awplus(config)# mls qos enable
awplus(config-if)# interface port1.0.7
awplus(config-if)# no wrr-queue egress-rate-limit queues 0 1
```

WRR-QUEUE WEIGHT

Syntax

```
wrr-queue weight weight queues queue_numbers
```

Parameters

weight
: Specifies the weight as a data ratio of a port's egress priority queue for WRR queuing. The range is 1 to 15.

queue_numbers
: Specifies one or multiple numbers of egress queues to use the WRR queuing method. The range is 0 to 7. Use a space to separate numbers. By default, all egress queues are specified to use Strict PQ.

Mode

Port Interface mode

Description

Use this command to set egress queues in the specified port to the WRR queuing method and specify the data ratios to queues. In WRR queuing, the port transmits packets in one queue based on the data ratio to the average size of packets transmitted for a certain period of time and then moves to next queue.

You must enable QoS on the switch to use this command. To enable QoS, see "MLS QOS ENABLE" on page 503.

Confirmation Command

"SHOW MLS QOS INTERFACE" on page 519

Example

This example specifies all queues of port 1.0.3 to WRR scheduling and data ratios to 10:10:5:5:2:2:1:1 to queues 7:6:5:4:3:2:1:0:

```
awplus# configure terminal
awplus(config)# mls qos enable
awplus(config)# interface port1.0.3
awplus(config-if)# wrr-queue weight 10 queues 7 6
awplus(config-if)# wrr-queue weight 5 queues 5 4
awplus(config-if)# wrr-queue weight 2 queues 3 2
awplus(config-if)# wrr-queue weight 1 queues 1 0
```

Chapter 22

DoS Defense Commands

The Denial of Service (DoS) defense commands are summarized in Table 83.

Table 83. DoS Commands

Command	Mode	Description
“DOS IPOPTIONS” on page 526	Port Interface	Enables the DoS IP options defense.
“DOS LAND” on page 528	Port Interface	Enables the DoS LAND defense.
“DOS PING-OF-DEATH” on page 530	Port Interface	Enables the DoS ping-of-death defense.
“DOS SMURF” on page 532	Port Interface	Enables the DoS Smurf defense.
“DOS SYNFLOOD” on page 534	Port Interface	Enables the DoS SYN flood defense.
“DOS TEARDROP” on page 536	Port Interface	Enables the DoS Teardrop defense.
“NO DOS IPOPTIONS” on page 538	Port Interface	Disables the DoS IP options defense.
“NO DOS LAND” on page 539	Port Interface	Disables the DoS LAND defense.
“NO DOS PING-OF-DEATH” on page 540	Port Interface	Disables the DoS ping-of-death defense.
“NO DOS SMURF” on page 541	Port Interface	Disables the DoS Smurf defense.
“NO DOS SYNFLOOD” on page 542	Port Interface	Disables the DoS SYN flood defense.
“NO DOS TEARDROP” on page 543	Port Interface	Disables the DoS Teardrop defense.
“SHOW DOS INTERFACE” on page 544	Privileged Exec	Displays the states of the DoS defenses.

DOS IPOPTIONS

Syntax

```
dos ipoptions action action
```

Parameter

action
: Specifies an action. The only action is “shutdown.” The switch temporarily shuts down the specified port for one minute when a DoS IP options attack is detected.

Mode

Port Interface mode

Description

Use this command to enable the defense against DoS IP options attacks. In DoS IP options attacks, attackers send large streams of packets with IP options to target networks and make network resources unavailable to legitimate traffic.

When the DoS IP options defense is enabled on a port, the switch counts the number of ingress IP packets containing IP options received on the port. If the number exceeds 20 packets per second, the switch temporarily shuts down the port for one minute.The port is enabled automatically after one minute passes.To enable a shut down port manually, use the NO SHUTDOWn command. See “NO SHUTDOWN” on page 254.

You can enable the DoS IP options defense on a per port basis. However, you *cannot* specify static or dynamic trunk groups, represented by “saX” and “poX” respectively, or ports that belong to a trunk.

The DoS IP options defense consumes 1 unit per port out of 256 resource units that are allocated to DoS defense on the switching chip that resides on the switch.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example enables the DoS IP options defense on port 1.0.1:

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

DOS LAND

Syntax

```
dos land action action
```

Parameter

action
: Specifies an action. The only action is “shutdown.” The switch temporarily shuts down the specified port for one minute when a DoS LAND attack is detected.

Mode

Port Interface mode

Description

Use this command to enable the defense against DoS Local Area Network Denial (LAND) attacks. In DoS LAND attacks, attackers use packets that are set to the same IP address for both source and destination addresses and make the device to reply to itself continuously.

When the DoS LAND defense is enabled on a port, the switch temporarily shuts down the port for one minute if the port receives a packet containing the same IP address for both source and destination addresses. The port is enabled automatically after one minute passes. To enable a shut down port manually, use the NO SHUTDOWN command. See “NO SHUTDOWN” on page 254.

You can enable the DoS LAND defense on a per port basis. However, you *cannot* specify static or dynamic trunk groups, represented by “saX” and “poX” respectively, or ports that belong to a trunk.

The DoS LAND defense consumes 1 unit per port out of 256 resource units that are allocated to the DoS defense on the switching chip that resides on the switch.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example enables the DoS LAND defense on port 1.0.5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# dos land action shutdown
```

DOS PING-OF-DEATH

Syntax

```
dos ping-of-death action action
```

Parameter

action
: Specifies an action. The only action is “shutdown.” The switch temporarily shuts down the specified port for one minute when a DoS ping-of-death attack is detected.

Mode

Port Interface mode

Description

Use this command to enable the defense against DoS ping-of-death attacks. In DoS ping-of-death attacks, attackers send fragmented packets that are greater than 65,565 bytes when they are reconstructed. Host machines that receive oversized IP packets may crash or be forced to reboot.

When the DoS ping-of-death defense is enabled on a port, the switch temporarily shuts down the port for one minute if the port receives a fragmented ICMP ECHO packet that is part of the packet greater than 65,447 bytes when the fragmented packets are reconstructed. The size of packets that the switch compares to 65,447 bytes is a packet except the IP header and ICMP header.

To enable a shut down port manually, use the NO SHUTDOWN command. See “NO SHUTDOWN” on page 254.

You can enable the DoS ping-of-death defense on a per port basis. However, you *cannot* specify static or dynamic trunk groups, represented by “saX” and “poX” respectively, or ports that belong to a trunk.

The DoS ping-of-death defense consumes 1 unit per port out of 256 resource units that are allocated to the DoS defense on the switching chip that reside on the switch.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example activates the DoS ping-of-death defense on port 1.0.5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# dos ping-of-death action shutdown
```

DOS SMURF

Syntax

```
dos smurf action action
```

Parameter

action
: Specifies an action. The only action is “shutdown.” The switch temporarily shuts down the specified port for one minute when a DoS Smurf attack is detected.

Mode

Port Interface mode

Description

Use this command to enable the defense against DoS Smurf attacks. In DoS Smurf attacks, attackers send a large number of ICMP echo request (ping) traffic with the IP address of an intended target system as the source address and IP broadcast address as the destination address. DoS Smurf attacks flood a system with broadcast ping messages.

When the DoS Smurf defense is enabled on a port, the switch temporarily shuts down the port for one minute if the port receives an ICMP echo request packet that contains the specified directed broadcast address. The port is enabled automatically after one minute passes. To enable a shut-down port manually, use the NO SHUTDOWN command. See “NO SHUTDOWN” on page 254.

You can enable the DoS Smurf defense on a per port basis. However, you *cannot* specify static or dynamic trunk groups, represented by “saX” and “poX” respectively, or ports that belong to a trunk.

The DoS Smurf defense consumes 1 unit per port out of 256 resource units are allocated to the DoS defense on the switching chip on the switch.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example enables the DoS Smurf defense on port 1.0.17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.17
awplus(config-if)# dos smurf broadcast 192.168.10.255 action
shutdown
```

DOS SYNFLOOD

Syntax

```
dos synflood action action
```

Parameter

action
: Specifies an action. The only action is “shutdown.” The switch temporarily shuts down the specified port for one minute when a DoS SYN flood attack is detected.

Mode

Port Interface mode

Description

Use this command to enable the defense against DoS SYN flood attacks. In DoS SYN flood attacks, attackers send a succession of TCP SYN requests to a target system and make system resources unavailable to legitimate traffic.

When the DoS SYN flood defense is enabled on a port, the switch counts the number of ingress TCP SYN packets received on the port. If the number exceeds 60 packets per second, the switch temporarily shuts down the port for one minute. The port is enabled automatically after one minute passes. To enable a shut down port manually, use the NO SHUTDOWN command. See “NO SHUTDOWN” on page 254.

You can enable the DoS SYN flood defense on a per port basis. However, you *cannot* specify static or dynamic trunk groups, represented by “saX” and “poX” respectively, or ports that belong to a trunk.

The DoS SYN flood defense consumes 1 unit per port out of 256 resource units that are allocated to the DoS defense on the switching chip that is located on the switch.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example enables the DoS SYN flood defense on port 1.0.5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# dos synflood action shutdown
```

DOS TEARDROP

Syntax

```
dos teardrop action action
```

Parameter

action
: Specifies an action. The only action is “shutdown.” The switch temporarily shuts down the specified port for one minute when a DoS SYN flood attack is detected.

Mode

Port Interface mode

Description

Use this command to enable the defense against DoS Teardrop attacks. In DoS Teardrop attacks, attackers send IP fragment packets that contain invalid overlapping values in the fragment offset field. When destination hosts attempt to reassemble the packets, the hosts may crash.

When the DoS Teardrop defense is enabled on a port, the switch temporarily shuts down the port for one minute if the port receives a fragmented packet with an invalid fragment offset value. The port is enabled automatically after one minute passes. To enable a shut-down port manually, use the NO SHUTDOWN command. See “NO SHUTDOWN” on page 254.

You can enable the DoS Teardrop defense on a per port basis. However, you *cannot* specify static or dynamic trunk groups, represented by “saX” and “poX” respectively, or ports that belong to a trunk.

The DoS Teardrop defense consumes 1 unit per port out of 256 resource units that are allocated to the DoS defense on the switching chip that resides on the switch.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example activates the DoS Teardrop defense on port 1.0.22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.22
awplus(config-if)# dos teardrop enable
```

NO DOS IPOPTIONS

Syntax

```
no dos ipoptions
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the DoS IP options defense on the ports.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example disables the DoS IP options defense on port 1.0.1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no dos ipoptions
```

NO DOS LAND

Syntax

```
no dos land enable
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the DoS LAND defense on a port.

Confirmation Command

"SHOW DOS INTERFACE" on page 544

Example

This example disables the DoS LAND defense on port 1.0.5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no dos land
```

NO DOS PING-OF-DEATH

Syntax

```
no dos ping-of-death
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the DoS ping-of-death defense.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example disables the DoS ping-of-death defense on port 1.0.20:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.20
awplus(config-if)# no dos ping-of-death
```

NO DOS SMURF

Syntax

```
no dos smurf
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the DoS Smurf defense.

Confirmation Command

"SHOW DOS INTERFACE" on page 544

Example

This example disables the defense on port 1.0.18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.18
awplus(config-if)# no dos smurf
```

NO DOS SYNFLOOD

Syntax

```
no dos synflood
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the DoS SYN flood defense.

Confirmation Command

“SHOW DOS INTERFACE” on page 544

Example

This example disables the DoS SYN flood defense on port 1.0.3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no dos synflood
```

NO DOS TEARDROP

Syntax

```
no dos teardrop
```

Parameters

None

Mode

Port Interface mode

Description

Use this command to disable the DoS Teardrop defense.

Confirmation Command

"SHOW DOS INTERFACE" on page 544

Example

This example disables the defense on port 1.0.5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no dos teardrop
```

SHOW DOS INTERFACE

Syntax

```
show dos interface port_ids
```

Parameter

port_ids
: Specifies a port ID or multiple port IDs. Use a comma (,) to separate port IDs and a hyphen (-) to indicate a range of port IDs.

Description

Use this command to display the configurations of the DoS defenses on the ports. The state of a defense is either enabled or disabled. See Figure 80 for an example of this command.

```
DoS settings for interface port1.0.9
---------------------------------------
Port status          : Enabled
synflood             : Disabled
smurf                : Disabled
land                 : Disabled
ipoptions            : Enabled
   Action            : Shutdown port
   Attacks detected  : 0
teardrop             : Disabled
ping-of-death        : Disabled
```

Figure 80. SHOW DOS INTERFACE Command

The fields are described in Table 84.

Table 84. SHOW DOS INTERFACE Command

Field	Description
Port status	Displays the status of the port as enabled or disabled.
synflood	Displays the status of the DoS SYN flood defense as enabled or disabled on the port.
smurf	Displays the status of the DoS SMURF defense as enabled or disabled on the port.

Table 84. SHOW DOS INTERFACE Command (Continued)

Field	Description
land	Displays the status of the DoS LAND defense as enabled or disabled on the port.
ipoptions	Displays the status of the DoS IP options defense as enabled or disabled on the port.
teardrop	Displays the status of the DoS tear-drop defense as enabled or disabled on the port.
ping-of-death	Displays the status of the DoS ping-of-death defense as enabled or disabled on the port.
Action	Displays the specified action when the DoS defense is enabled.
Attacks detected	Displays the number of the DoS attacks detected on the port when the DoS defense is enabled.

Examples

This example displays the DoS defense configurations for all of the ports:

```
awplus> enable
awplus# show dos interface
```

This example displays the DoS defense states for ports 1.0.21 and 1.0.22:

```
awplus> enable
awplus# show dos interface port1.0.21,port1.0.22
```

Command Index

P

Q

R

S

T

U

V

W