Franchise 2.5 CLI Commands

Rev. 1.0

August 18, 2011, Customer Version

CONFIDENTIAL

Document Classification: Restricted Information

Document Conventions

	**Note:** Provides related information or information of special importance.
	**Caution:** Indicates potential damage to hardware or software, or loss of data.
	**Warning:** Indicates a risk of personal injury.

Document Status

Doc Status: For Customer Review	

Table of Contents

1 Preface

About this Document

This CLI Reference Guide describes how to use the CLI and a list of the CLI commands and their arguments.

The CLI commands described in this document are organized according to feature groups in separate sections.

This section describes how to use the CLI. It contains the following topics:

CLI Command Modes

To configure devices, the CLI is divided into various command modes. Each command mode has its own set of specific commands. Entering a question mark "?" at the console prompt displays a list of commands available for that particular command mode.

A specific command, which varies from mode to mode, is used to navigate from one mode to another. The standard order to access the modes is as follows: *User EXEC* mode, *Privileged EXEC* mode, *Global Configuration* mode, and *Interface Configuration* modes.

When starting a session, the initial mode for non-privileged users is the User EXEC mode. Only a limited subset of commands is available in the User EXEC mode. This level is reserved for tasks that do not change the configuration.

Privileged users enter the Privileged EXEC mode directly using a password. This mode provides access to the device Configuration modes.

The modes are described below.

User EXEC Mode

After logging into the device, the user is automatically in *User EXEC* command mode unless the user is defined as a privileged user. In general, the *User EXEC* commands enable the user to perform basic tests, and display system information.

The user-level prompt consists of the device "host name" followed by the angle bracket (>).

```
console>
```

The default host name is "console" unless it has been changed using the **hostname** command in the *Global Configuration* mode.

Privileged EXEC Mode

Privileged access is password-protected to prevent unauthorized use, because many of the privileged commands set operating system parameters: The password is not displayed on the screen and is case sensitive.

Privileged users enter directly into the *Privileged EXEC* mode.

Use **disable** to return to the *User EXEC* mode.

Global Configuration Mode

Global Configuration mode commands apply to features that affect the system as a whole, rather than just a specific interface.

To enter the *Global Configuration* mode, enter **configure** in the Privileged EXEC mode, and press <Enter>.

The *Global Configuration* mode prompt is displayed.

```
console(config)#
```

Use **exit**, **end** or **ctrl/z** to return to the Privileged EXEC mode.

Interface Configuration Modes

Commands in the following modes perform specific interface operations:

- **Line Interface** — Contains commands to configure the management connections. These include commands such as line speed, timeout settings, etc. The *Global Configuration* mode command **line** is used to enter the *Line Configuration command* mode.
- **VLAN Database** — Contains commands to create a VLAN as a whole. The Global Configuration mode command **vlan database** is used to enter the *VLAN Database Interface Configuration* mode.
- **Management Access List** — Contains commands to define management access-lists. The *Global Configuration* mode command management access-list is used to enter the *Management Access List Configuration* mode.
- **Port Channel** — Contains commands to configure port-channels, for example, assigning ports to a VLAN or port-channel. The *Global Configuration* mode command interface **port-channel** is used to enter the *Port Channel Interface Configuration* mode.
- **SSH Public Key-Chain** — Contains commands to manually specify other device SSH public keys. The *Global Configuration* mode command crypto key pubkey-chain **ssh** is used to enter the *SSH Public Key-chain Configuration* mode.
- **Interface** — Contains commands that configure the interface. The *Global Configuration* mode command **interface** is used to enter the *Interface Configuration* mode.

Starting the CLI

The switch can be managed over a direct connection to the switch console port, or via a Telnet connection. The switch is managed by entering command keywords and parameters at the prompt. Using the switch CLI commands is similar to entering commands on a UNIX system.

If access is via a Telnet connection, ensure the device has an IP address defined, corresponding management access is granted, and the workstation used to access the device is connected to the device prior to using CLI commands.

Accessing the CLI from the Console Line

1. Start the device and wait until the startup procedure is complete. The User Exec mode is entered, and the prompt "console>" is displayed.
2. Configure the device and enter the necessary commands to complete the required tasks.
3. When finished, exit the session with the **quit** or **exit** command.

Accessing the CLI from Telnet

1. Enter **telnet** and the IP address of the device. A User Name prompt is displayed.
2. Enter the User Name and Password. You are in the Privileged Exec mode.

3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, exit the session with the quit or exit command.

When another user is required to log onto the system, the **login** command is entered in the Privileged EXEC command mode,. This effectively logs off the current user and logs on the new user.

CLI Command Conventions

The following table describes the command syntax conventions.

Conventions	Description
[ ]	In a command line, square brackets indicates an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated by the | character. One option must be selected. For example: **flowcontrol {auto|on|off}** means that for the **flowcontrol** command either **auto**, **on** or **off** must be selected.
Italic font	Indicates a parameter.
<Enter>	Any individual key on the keyboard. For example click **<Enter>**.
Ctrl+F4	Any combination keys pressed simultaneously on the keyboard.
`Screen Display`	Indicates system messages and prompts appearing on the console.
all	When a parameter is required to define a range of ports or parameters and **all** is an option, the default for the command is **all** when no parameters are defined. For example, the command **interface range port-channel** has the option of either entering a range of channels, or selecting **all**. When the command is entered without a parameter, it automatically defaults to **all**.
interface-id	This indicates a port, VLAN or LAG. The syntax for interface_id is as follows: {***port_type***}*port-number* |{***vlan***} *vlan-id* | {***port-channel***} *LAG-number*
port_type	Port type can be one of the following depending on the port types on the device: ■ 10/100 Mbps - Fastethernet can be shortened to fa, as in fa1 ■ 1000 Gbps Gigabitethernet can be shortened to GE or gi, as in GE 1 or gi1. ■ 10G Gbps - 10 Gigabitethernet can be shortened to FE, as in FE 1.

Entering Commands

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "**show interfaces status gi1/0/5**" **show**, **interfaces** and **status** are keywords, **gi** is an argument that specifies the interface type, and **1/0/5** is an argument that specifies the port.

To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
console(config)# username admin password smith
```

Help information can be displayed in the following ways:

- **Keyword Lookup** — The character ? is entered in place of a command. A list of all valid commands and corresponding help messages are displayed.

- **Partial Keyword Lookup** — A command is incomplete and the character ? is entered in place of a parameter. The matched parameters for this command are displayed.

The following describes features that assist in using the CLI:

Terminal Command Buffer

Every time a command is entered in the CLI, it is recorded on an internally managed Command History buffer. Commands stored in the buffer are maintained on a First In First Out (FIFO) basis.These commands can be recalled, reviewed, modified, and reissued. This buffer is not preserved across device resets. The keys that can be used to access the history buffer are described in Table 2.

By default, the history buffer system is enabled, but it can be disabled at any time. For information about the command syntax to enable or disable the history buffer, see the **history** command.

There is a standard default number of commands that are stored in the buffer. The standard number of 10 commands can be increased to 256. By configuring 0, the effect is the same as disabling the history buffer system. For information about the command syntax for configuring the command history buffer, see the **history size** command.

To display the history buffer, see **show history** command.

Negating the Effect of Commands

For many configuration commands, the prefix keyword "no" can be entered to cancel the effect of a command or reset the configuration to the default value. This guide describes the negation effect for all applicable commands.

Command Completion

If the command entered is incomplete, invalid, or has missing or invalid parameters, an appropriate error message is displayed.

To complete an incomplete command, press the <Tab> button. If the characters already entered are not enough for the system to identify a single matching command, press "?" to display the available commands matching the characters already entered.

Incorrect or incomplete commands are automatically re-entered next to the cursor. If a parameter must be added, the parameter can be added to the basic command already displayed next to the cursor. The following example indicates that the command interface requires a missing parameter.

```
(config)#interface
%missing mandatory parameter
(config)#interface
```

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in entering the CLI commands.

The following table describes these shortcuts:

Table 2: Keyboard Keys

Keyboard Key	Description
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow key	Returns the most recent commands from the history buffer after recalling commands with the up arrow key. Repeating the key sequence will recall successively more recent commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any mode.
Backspace key	Moves the cursor back one space.
Up-arrow key	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.

2 User Interface Commands

2.1 enable

The **enable** EXEC mode command enters the Privileged EXEC mode.

Syntax

enable [*privilege-level*]

Parameters

privilege-level—Specifies the privilege level at which to enter the system. (Range: 1, 7, 15)

Default Configuration

The default privilege level is 15.

Command Mode

EXEC mode

Example

The following example enters privilege level 7.

```
switchxxxxxx#  enable 7
enter password:**********
switchxxxxxx#Accepted
```

The following example enters privilege level 15.

```
switchxxxxxx#  enable
enter password:**********
switchxxxxxx#Accepted
```

2.2 disable

The **disable** Privileged EXEC mode command leaves the Privileged EXEC mode and returns to the User EXEC mode.

Syntax

disable [*privilege-level*]

Parameters

privilege-level—Reduces the privilege level to the specified privileged level. If privilege level is left blank, the level is reduce to 1.

Default Configuration
The default privilege level is 1.

Command Mode
Privileged EXEC mode

Example
The following example returns the user to user level 7.

```
switchxxxxxx# disable 7
switchxxxxxx#
```

2.3 login
The **login** EXEC mode command enables changing the user that is logged in. When this command is logged in, the user is prompted for a username/password.

Syntax
login

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example enters Privileged EXEC mode and logs in with the required username ‘bob’.

```
switchxxxxxx#  login
User Name:bob
Password:*****
switchxxxxxx#
```

2.4 configure
The **configure** Privileged EXEC mode command enters the Global Configuration mode.

Syntax
configure [***terminal***]

Parameters
terminal—Enter the Global Configuration mode with or without the keyword terminal.

Command Mode
Privileged EXEC mode

Example
The following example enters Global Configuration mode.

```
switchxxxxxx# configure
switchxxxxxx(config)#
```

2.5 exit (Configuration)
The **exit** command exits any mode and brings the user to the next higher mode in the CLI mode hierarchy.

Syntax
exit

Parameters
N/A

Default Configuration
N/A

Command Mode
All.

Examples
The following examples change the configuration mode from Interface Configuration mode to Privileged EXEC mode.

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

2.6 exit (EXEC)
The **exit** EXEC mode command closes an active terminal session by logging off the device.

Syntax
exit

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example closes an active terminal session.

```
switchxxxxxx#  exit
```

2.7 end
The **end** command ends the current configuration session and returns to the Privileged EXEC mode.

Syntax
end

Parameters
N/A

Default Configuration
N/A

Command Mode
All

Example
The following example ends the Global Configuration mode session and returns to the Privileged EXEC mode.

```
switchxxxxxx(config)# end
switchxxxxxx#
```

2.8 help
The **help** command displays a brief description of the Help system.

Syntax
help

Parameters
N/A

Default Configuration
N/A

Command Mode
All

Example

The following example describes the Help system.

```
switchxxxxxx# help

Help may be requested at any point in a command by entering a question
mark '?'. If nothing matches the currently entered incomplete command, the
help list is empty. This indicates that there is no command matching the
input as it currently appears. If the request is within a command, press
the Backspace key and erase the entered characters to a point where the
request results in a match.

Help is provided when:

1. There is a valid command and a help request is made for entering a
parameter or argument (e.g. 'show ?'). All possible parameters or
arguments for the entered command are then displayed.

2. An abbreviated argument is entered and a help request is made for
arguments matching the input (e.g. 'show pr?').
```

2.9 history

The **history** Line Configuration mode command enables saving commands that have been entered. Use the **no** form of this command to disable the command.

Syntax

history

no history

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Line Configuration mode

User Guidelines

This command enables saving user-entered commands for a specified line. You can return to previous lines by using the up or down arrows.

It is effective from the next time that the user logs in via console/telnet/ssh.

The following are related commands:

- Use the terminal history size EXEC mode command to enable or disable this command for the current terminal session.
- Use the history size Line Configuration mode command to set the size of the command history buffer.

Example

The following example enables the command for Telnet.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history
```

2.10 history size

The **history size** Line Configuration mode command changes the maximum number of user commands that are saved in the history buffer for a particular line. Use the **no** form of this command to reset the command history buffer size to the default value.

Syntax

history size *number-of-commands*

no history size

Parameters

number-of-commands—Specifies the number of commands the system records in its history buffer. (Range: 10–207)

Default Configuration

The default command history buffer size is 10 commands.

Command Mode

Line Configuration mode

User Guidelines

This command configures the command history buffer size for a particular line. It is effective from the next time that the user logs in via console/telnet/ssh.

Use the **terminal history size** EXEC mode command to configure the command history buffer size for the current terminal session.

The allocated command history buffer is per terminal user, and is taken from a shared buffer. If there is not enough space available in the shared buffer, the command history buffer size cannot be increased above the default size.

Example

The following example changes the command history buffer size to 100 entries for Telnet.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# history size 100
```

2.11 terminal history

The **terminal history** EXEC mode command enables the command history function for the current terminal session, meaning it is not stored in the Running Configuration file. Use the **no** form of this command to disable the command.

Syntax

terminal history

terminal no history

Default Configuration

The default configuration for all terminal sessions is defined by the history Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the history Line Configuration mode command.

This command is effective immediately.

Example

The following example disables the command history function for the current terminal session.

```
switchxxxxxx#  terminal no history
```

2.12 terminal history size

The **terminal history size** EXEC mode command changes the command history buffer size for the current terminal session, meaning it is not stored in the Running Configuration file. Use the **no** form of this command to reset the command history buffer size to the default value.

Syntax

terminal history size *number-of-commands*

terminal no history size

Parameters

number-of-commands—Specifies the number of commands the system maintains in its history buffer. (Range: 10–207)

Default Configuration

The default configuration for all terminal sessions is defined by the history size Line Configuration mode command.

Command Mode

EXEC mode

User Guidelines

The **terminal history size** EXEC command changes the command history buffer size for the current terminal session. Use the history Line Configuration mode command to change the default history buffer size.

The maximum number of commands in all buffers is 207.

Example

The following example sets the command history buffer size to 20 commands for the current terminal session.

```
switchxxxxxx#terminal history size 20
```

2.13 terminal datadump

The **terminal datadump** EXEC mode command enables dumping all the output of a show command without prompting. Use the **no** form of this command to disable dumping.

Syntax

terminal datadump

no terminal datadump

Parameters

N/A

Default Configuration

When printing, dumping is disabled and printing is paused every 24 lines.

Command Mode

EXEC mode

User Guidelines

By default, a **More** prompt is displayed when the output contains more than 24 lines. Pressing the **Enter** key displays the next line; pressing the **Spacebar** displays the next screen of output.

The **terminal datadump** command enables dumping all output immediately after entering the show command by removing the pause.

The width is currently not limited (previously the limit was 77 chars), and the width of the line being printed on the terminal is based on the terminal itself.

This command is relevant only for the current session.

Example

The following example dumps all output immediately after entering a show command.

```
switchxxxxxx#  terminal datadump
```

2.14 debug-mode

The **debug-mode** Privileged EXEC mode command mode switches to debug mode.

Syntax

debug-mode

Parameters

N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example enters Debug mode.

```
switchxxxxxx# debug-mode
```

2.15 show history
The **show history** EXEC mode command lists commands entered in the current session.

Syntax
show history

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

User Guidelines
The buffer includes executed and unexecuted commands.

Commands are listed from the first to the most recent command.

The buffer remains unchanged when entering into and returning from configuration modes.

Example
The following example displays all the commands entered while in the current Privileged EXEC mode.

```
switchxxxxxx# show version
SW version 3.131 (date 23-Jul-2005 time 17:34:19)
HW version 1.0.0
switchxxxxxx# show clock
15:29:03 Jun 17 2005
switchxxxxxx# show history
show version
show clock
show history
```

```
3 commands were logged (buffer size is 10)
```

2.16 show privilege

The **show privilege** EXEC mode command displays the current privilege level.

Syntax

show privilege

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays the privilege level for the user logged on.

```
switchxxxxxx# show privilege
Current privilege level is 15
```

2.17 do

The **do** command executes an EXEC-level command from Global Configuration mode or any configuration submode.

Syntax

do *command*

Parameters

command—Specifies the EXEC-level command to execute.

Command Mode

All configuration modes

Example

The following example executes the **show vlan** Privileged EXEC mode command from Global Configuration mode.

Example

```
switchxxxxxx(config)# do show vlan
Vlan  Name        Ports                  Type         Authorization
---- ----       ---------------------    --------     -------------
```

```
 1    1           fe1/0/11-39,Po1,Po2,         other        Required
 2    2           fe1/0/11                     dynamicGvrp  Required
 10   v0010       fe1/0/11                     permanent    Not Required
 11   V0011       fe1/0/11,fe1/0/13                 permanent    Required
 20   20          fe1/0/11                     permanent    Required
 30   30          fe1/0/11,fe1/0/13                 permanent    Required
 31   31          fe1/0/11                     permanent    Required
 91   91          fe1/0/11,fe1/0/14                 permanent    Required
 4093 guest-vlan  fe1/0/11,fe1/0/13                 permanent    Guest
switchxxxxxx(config)#
```

2.18 banner exec

Use the **banner exec** Global Configuration mode command to specify and enable a message to be displayed after a successful logon. Use the **no** form of this command to delete the existing EXEC banner.

Syntax

banner exec *d message-text d*

no banner exec

Parameters

- **d**—Delimiting character of user's choice—a pound sign (**#**), for example. You cannot use the delimiting character in the banner message.
- **message-text**—The message must start in a new line. You can enter multi-line messages. You can include tokens in the form of **$(token)** in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 2000 characters (after every 510 characters, press **<Enter>** to continue).

Default Configuration

Disabled (no EXEC banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of **$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information Displayed in the Banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.

Token	Information Displayed in the Banner
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the **no banner exec** Line Configuration command to disable the Exec banner on a particular line or lines.

Example

The following example sets an EXEC banner that uses tokens. The percent sign (**%**) is used as a delimiting character. Note that the **$(token)** syntax is replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner exec %
Enter TEXT message. End with the character '%'.
$(bold)Session activated.$(bold) Enter commands at the prompt.
%
When a user logs on to the system, the following output is displayed:
Session activated. Enter commands at the prompt.
```

2.19 banner login

Use the **banner login** command in Global Configuration mode to specify a message to be displayed before the username and password login prompts. This banner is applied automatically on all the CLI interfaces: Console, Telnet and SSH and also on the WEB GUI. Use the **no** form of this command to delete the existing login banner.

Syntax

banner login *d message-text d*

no banner login

Parameters

- **d**—Delimiting character of user's choice—a pound sign (**#**), for example. You cannot use the delimiting character in the banner message.
- **message-text**—Message text. The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of **$(token)** in the message text. Tokens are replaced with the corresponding configuration variable (see User Guidelines). The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration

Disabled (no Login banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

Use tokens in the form of **$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.
$(bold)	Indicates that the next text is a bold text. Using this token again indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the **no banner login** Line Configuration command to disable the Login banner on a particular line or lines.

Example

The following example sets a Login banner that uses tokens. The percent sign (**%**) is used as a delimiting character. Note that the **$(token)** syntax is replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner login %
Enter TEXT message. End with the character '%'.
You have entered $(hostname).$(domain)
%
When the login banner is executed, the user will see the following banner:
You have entered host123.ourdomain.com
```

2.20 banner motd

Use the **banner motd** command in Global Configuration mode to specify and enable a message-of-the-day banner. This message is displayed before the login banner. Use the **no** form of this command to delete the existing MOTD banner.

Syntax

banner motd *d message-text d*

no banner motd

Parameters

- **d**—Delimiting character of user's choice—a pound sign (**#**), for example. You cannot use the delimiting character in the banner message.
- **message-text**—The message must start on a new line. You can enter multi-line messages. You can include tokens in the form of **$(token)** in the message text. Tokens are replaced with the corresponding configuration variable. Tokens are described in the User Guidelines. The message can contain up to 2000 characters (after every 510 characters, you must press <Enter> to continue).

Default Configuration

Disabled (no MOTD banner is displayed).

Command Mode

Global Configuration mode

User Guidelines

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

When a user connects to a device, the message-of-the-day (MOTD) banner appears first, followed by the login banner and prompts. After the user logs in to the device, the EXEC banner is displayed.

Use tokens in the form of **$(token)** in the message text to customize the banner. The tokens are described in the table below:

Token	Information displayed in the banner
$(hostname)	Displays the host name for the device.
$(domain)	Displays the domain name for the device.
$(bold)	Indicates that the next text is a bold text. Using this token again to indicates the end of the bold text.
$(inverse)	Indicates that the next text is an inverse text. Using this token again indicates the end of the inverse text.
$(contact)	Displays the system contact string.
$(location)	Displays the system location string.
$(mac-address)	Displays the base MAC address of the device.

Use the **no banner motd** Line Configuration command to disable the MOTD banner on a particular line or lines.

Example

The following example sets an MOTD banner that uses tokens. The percent sign (**%**) is used as a delimiting character. Note that the **$(token)** syntax is replaced by the corresponding configuration variable.

```
switchxxxxxx(config)# banner motd %
Enter TEXT message. End with the character '%'.
$(bold)Upgrade$(bold) to all devices begins at March 12
%
```

```
When the login banner is executed, the user will see the following banner:
Upgrade to all devices begins at March 12
```

2.21 exec-banner

Use the **exec-banner** command in Line Configuration mode to enable the display of exec banners. Use the **no** form of this command to disable the display of exec banners.

Syntax

exec-banner

no exec-banner

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Line Configuration mode

Example

```
switchxxxxxx# configure
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# exec-banner
switchxxxxxx(config-line)# exit
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# exec-banner
switchxxxxxx(config-line)# exit
switchxxxxxx(config)# line ssh
switchxxxxxx(config-line)# exec-banner
```

2.22 login-banner

Use the **login-banner** command in Line Configuration mode to enable the display of login banners. Use the **no** form of this command to disable the display of login banners.

Syntax

login-banner

no login-banner

Parameters

This command has no arguments or keywords.

Default Configuration
Enabled

Command Mode
Line Configuration mode

Example

```
switchxxxxxx# configure
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login-banner
switchxxxxxx(config-line)# exit
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# login-banner
switchxxxxxx(config-line)# exit
switchxxxxxx(config)# line ssh
switchxxxxxx(config-line)# login-banner
```

2.23 motd-banner

Use the **motd-banner** command in Line Configuration mode to enable the display of message-of-the-day banners. Use the **no** form of this command to disable the display of MOTD banners.

Syntax
motd-banner

no motd-banner

Parameters
This command has no arguments or keywords.

Default Configuration
Enabled

Command Mode
Line Configuration mode

Example

```
switchxxxxxx# configure
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# motd-banner
switchxxxxxx(config-line)# exit
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# motd-banner
```

```
switchxxxxxx(config-line)# exit
switchxxxxxx(config)# line ssh
switchxxxxxx(config-line)# motd-banner
```

2.24 show banner

Use the **show banner** commands in EXEC mode to display the banners that have been defined.

Syntax

>show banner motd

show banner login

show banner exec

Parameters

This command has no arguments or keywords.

Command Mode

EXEC mode

Examples

```
switchxxxxxx# show banner motd
Banner: MOTD
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
10000 giga ports switch
switchxxxxxx# show banner login
-------------------------------------------------------------
Banner: Login
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
switchxxxxxx# show banner exec
-------------------------------------------------------------
Banner: EXEC
Line SSH: Enabled
Line Telnet: Enabled
Line Console: Enabled
You have logged on
```

3 Macro Commands

3.1 macro name

Use the **macro name** Global Configuration mode command to define a macro. There are two types of macros that can be defined:

- Global macros define a group of CLI commands that can be run at any time.
- Smartport macros are associated with Smartport types (Section 45 "Smartport Commands"). For each Smartport macro there must be an anti macro (a macro whose name is concatenated with **no_**). The anti macro reverses the action of the macro.

If a macro with this name already exists, it overrides the previously-defined one.

Use the **no** form of this command to delete the macro definition.

Syntax

macro name *[macro-name]*

no macro name *[macro-name]*

Parameters

macro-name—Name of the macro. Macro names are case sensitive.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

A macro is a script that contains CLI commands and is assigned a name by the user. It can contain up to 3000 characters and 200 lines.

Keywords

Macros may contain keywords (parameters). The following describes keywords:

- A macro can contain up to three keywords.
- All matching occurrences of the keyword are replaced by the corresponding value specified in macro apply.
- Keyword matching is case-sensitive
- Applying a macro with keywords does not change the state of the original macro definition.

User Feedback

The behavior of a macro command requiring user feedback is the same as if the command is entered from terminal: it sends its prompt to the terminal and accepts the user reply.

Creating a Macro

Use the following guidelines to create a macro:

- Use **macro name** to create the macro with the specified name.
- Enter one macro command per line.
- Use the **@** character to end the macro.

- Use the **#** character at the beginning of a line to enter a comment in the macro.
  In addition, # is used to identify certain preprocessor commands that can only be used within a macro. There are two possible preprocessor commands:
  - **#macro key description -** Each macro can be configured with up to 3 keyword/description pairs. The keywords and descriptions are displayed in the GUI pages when the macro is displayed.
    The syntax for this preprocessor command is as follows:
    #macro key description $*keyword1 description1 $keyword2 description2 $keyword3 description3*
    A keyword must be prefixed with '$'.
  - **#macro keywords** - This instruction enables the device to display the keywords as part of the CLI help. It accepts up to 3 keywords. The command creates a CLI help string with the keywords for the macro. The help string will be displayed if help on the macro is requested from the **macro apply** and **macro global** commands. The GUI also uses the keywords specified in the command as the parameter names for the macro. See Example 2 and 3 below for a description of how this command is used in the CLI.
    The syntax for this preprocessor command is as follows:
    #macro keywords $*keyword-1* $*keyword2* $*keyword3*
    where $keyword-n is the name of the keyword.

Editing a Macro

Macros cannot be edited. Modify a macro by creating a new macro with the same name as the existing macro. The newer macro overwrites the existing macro.

The exceptions to this are the built-in macros and corresponding anti-macros for the Smartport feature. You cannot override a Smartport macro. To change a Smartport macro, create a new macro (my_macro) and an anti macro (no_my_macro) and associate it with the Smartport type using macro auto user smartport macro.

Scope of Macro

It is important to consider the scope of any user-defined macro. Because of the potential hazards of applying unintended configurations, do not change configuration modes within the macro by using commands such as **exit**, **end**, or **interface** *interface-id*. With a few exceptions, there are other ways of executing macros in the various configuration modes. Macros may be executed in Privileged Exec mode, Global Configuration mode, and Interface Configuration mode (when the interface is NOT a VLAN.)

Examples

Example 1 -The following example shows how to create a macro that configures the duplex mode of a port.

```
switchxxxxxx(config)#  macro name dup
Enter macro commands one per line. End with the character '@'.
#macro description dup
duplex full
negotiation
@
```

Example 2 -The following example shows how to create a macro with the parameters: DUPLEX and SPEED. When the macro is run, the values of DUPLEX and SPEED must be provided by the user. The **#macro keywords** command enables the user to receive help for the macro as shown in Example 3.

```
switchxxxxxx(config) #  macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex $DUPLEX
no negotiation
speed $SPEED
#macro keywords $DUPLEX $SPEED
@
```

Example 3 -The following example shows how to display the keywords using the help character ? (as defined by the **macro keywords** command above) and then run the macro on the port. The **#macro keywords** command entered in the macro definition enables the user to receive help for the macro, as shown after the words e.g. below.

```
switchxxxxxx(config-if)#interface gi1
switchxxxxxx(config-if)#macro apply duplex ?
    WORD <1-32>  Keyword to replace with value e.g. $DUPLEX, $SPEED
    <cr>
switchxxxxxx(config-if)#macro apply duplex $DUPLEX ?
    WORD<1-32>  First parameter value
    <cr>
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED ?
    WORD<1-32>  Second parameter value
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full $SPEED 100
```

3.2 macro apply

Use the **macro apply/trace** Interface Configuration command to either:

- Apply a macro to an interface without displaying the actions being performed
- Apply a macro to the interface while displaying the actions being performed

Syntax

macro {***apply*** | ***trace***} *macro-name [parameter-name1 {value}] [parameter-name2 {value}] [parameter-name3 {value}*]

Parameters

- **apply**—Apply a macro to the specific interface.
- **trace**—Apply and trace a macro to the specific interface.
- **macro-name**—Name of the macro.
- **parameter-name** *value*—(Optional) For each parameter defined in the macro, specify its name and value. You can enter up to three parameter-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the parameter name in the macro are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

The **macro apply** command hides the commands of the macro from the user while it is being run. The **macro trace** command displays the commands along with any errors which are generated by them as they are executed. This is used to debug the macro and find syntax or configuration errors.

When you run a macro, if a line in it fails because of a syntax or configuration error, the macro continues to apply the remaining commands to the interface.

If you apply a macro that contains parameters in its commands, the command fails if you do not provide the values for the parameters. You can use the **macro apply** *macro-name* with a **'?'** to display the help string for the macro keywords (if you have defined these with the **#macro keywords** preprocessor command).

Parameter (keyword) matching is case sensitive. All matching occurrences of the parameter are replaced with the provided value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

When you apply a macro to an interface, the switch automatically generates a macro description command with the macro name. As a result, the macro name is appended to the macro history of the interface. The show parser macro command displays the macro history of an interface.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When a macro is applied to an interface range, it is applied sequentially to each interface within the range. If a macro command fails on one interface, it is nonetheless attempted to be applied and may fail or succeed on the remaining interfaces.

Examples.

Example 1 - The following is an example of a macro being applied to an interface with the trace option.

```
switchxxxxxx(config) #  interface fe1/0/12
switchxxxxxx<config-if> #   macro trace dup $DUPLEX full $SPEED 100
  Applying command…  'duplex full'
  Applying command…  'speed 100'
switchxxxxxx<config-if> #
```

Example 2 - The following is an example of a macro being applied without the trace option.

```
switchxxxxxx(config) # interface fe1/0/12
switchxxxxxx<config-if> #  macro apply dup $DUPLEX full $SPEED 100
switchxxxxxx<config-if> #
```

Example 3 - The following is an example of an incorrect macro being applied.

```
switchxxxxxx(config-if)#macro trace dup
Applying command...'duplex full'
Applying command...'speed auto'
% bad parameter value
```

3.3 macro description

Use the **macro description** Interface Configuration mode command to append a description, for example, a macro name, to the macro history of an interface. Use the **no** form of this command to clear the macro history of an interface. When the macro is applied to an interface, the switch automatically generates a macro description command with the macro name. As a result, the name of the macro is appended to the macro history of the interface.

Syntax

macro description *text*

no macro description

Parameters

text—Description text. The text can contain up to 160 characters. The text must be double quoted if it contains multiple words.

Default Configuration

The command has no default setting.

Command Mode

Interface Configuration mode

User Guidelines

When multiple macros are applied on a single interface, the description text is a concatenation of texts from a number of previously-applied macros.

To verify the settings created by this command, run **show parser macro**.

Example

```
switchxxxxxx(config)#interface fe1/0/12
switchxxxxxx(config-if)#macro apply dup
switchxxxxxx(config-if)#exit
switchxxxxxx(config)#interface fe1/0/13
switchxxxxxx(config-if)#macro apply duplex $DUPLEX full SPEED 100
switchxxxxxx(config-if)#macro description dup
switchxxxxxx(config-if)#macro description duplex
switchxxxxxx(config-if)#end
switchxxxxxx#show parser macro description
Global Macro(s):
Interface      Macro Description(s)
------------   -------------------------------------------------
fe1/0/12             dup
fe1/0/13             duplex | dup | duplex
-----------------------------------------------------------------
switchxxxxxx#configure
```

```
switchxxxxxx(config)#interface fe1/0/12
switchxxxxxx(config-if)#no macro description
switchxxxxxx(config-if)#end
switchxxxxxx#show parser macro description
Global Macro(s):
Interface      Macro Description(s)
---------      ------------------------------------------------------
gi3            duplex | dup | duplex
------------------------------------------------------------------
switchxxxxxx#
```

3.4 macro global

Use the **macro global** Global Configuration command to apply a macro to a switch (with or without the trace option).

Syntax

macro global {***apply*** | ***trace***} *macro-name [parameter-name1 {value}] [parameter-name2 {value}] [parameter -name3 {value}*]

Parameters

- **apply**—Apply a macro to the switch.
- **trace**—Apply and trace a macro to the switch.
- **macro-name**—Specify the name of the macro.
- **parameter-name** *value*—(Optional) Specify the parameter values required for the switch. You can enter up to three parameter-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the parameters are replaced with the corresponding value.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a large string, is considered a match and replaced by the corresponding value.

If you apply a macro that contains keywords in its commands, the command fails if you do not specify the proper values for the keywords when you apply the macro. You can use this command with a '?' to display the help string for the macro keywords. You define the keywords in the help string using the preprocessor command **#macro keywords** when you define a macro.

When you apply a macro in Global Configuration mode, the switch automatically generates a global macro description command with the macro name. As a result, the macro name is appended to the global macro history. Use **show parser macro** to display the global macro history.

Example.

The following is an example of a macro being defined and then applied to the switch with the trace option.

```
switchxxxxxx(config)#  macro name console-timeout
Enter macro commands one per line. End with the character '@'.
line console
exec-timeout $timeout-interval
@
switchxxxxxx(config)#  macro global trace console-timeout $timeout-interval 100
  Applying command…  'line console'
  Applying command…  'exec-timeout 100'
switchxxxxxx(config)#
```

3.5 macro global description

Use the **macro global description** Global Configuration command to enter a description which is used to indicate which macros have been applied to the switch. Use the **no** form of this command to remove the description.

Syntax

macro global description *text*

no macro global description

Parameters

text—Description text. The text can contain up to 160 characters.

Default Configuration

The command has no default setting.

Command Mode

Global Configuration mode

User Guidelines

When multiple global macros are applied to a switch, the global description text is a concatenation of texts from a number of previously applied macros.

You can verify your settings by entering the **show parser macro description** privileged EXEC mode command.

Examples

```
switchxxxxxx(conf)#  macro global description "set console timeout interval"
```

3.6 show parser macro

Use the **show parser macro** User EXEC mode command to display the parameters for all configured macros or for one macro on the switch.

Syntax

show parser macro [*{**brief** | **description [interface** interface-id] | **name** macro-name}*]

Parameters

- **brief**—Display the name of all macros.
- **description** [**interface** *interface-id*]—Display the macro descriptions for all interfaces or if an interface is specified, display the macro descriptions for that interface.
- **name** *macro-name*—Display information about a single macro identified by the macro name.

Command Mode

User EXEC mode

Examples

Example 1 - This is a partial output example from the **show parser macro** command.

```
switchxxxxxx#  show parser macro
Total number of macros = 6
----------------------------------------------------------------
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
<output truncated>
----------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access
<output truncated>
```

Example 2 - This is an example of output from the **show parser macro name** command.

```
switchxxxxxx#  show parser macro standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
```

```
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

Example 3 - This is an example of output from the **show parser macro brief** command.

```
switchxxxxxx#  show parser macro brief
default global : cisco-global
default interface: cisco-desktop
default interface: cisco-phone
default interface: cisco-switch
default interface: cisco-router
customizable : snmp
```

This is an example of output from the **show parser macro description** command.

```
switchxxxxxx#  show parser macro description
Global Macro(s): cisco-global
```

Example 4 - This is an example of output from the **show parser macro description interface** command.

```
switchxxxxxx#  show parser macro description interface fe1/0/12
Interface Macro Description
---------------------------------------------------------------
fe1/0/12 this is test macro
---------------------------------------------------------------
```

4 System Management Commands

4.1 ping

Use the **ping** EXEC mode command to send ICMP echo request packets to another node on the network.

Syntax

ping [ip] *{ipv4-address | hostname} [**size** packet_size] [**count** packet_count] [**timeout** time_out]*

ping ipv6 *{ipv6-address | hostname} [**size** packet_size] [**count** packet_count] [**timeout** time_out]*

Parameters

- **ip**—Use IPv4 to check the network connectivity.
- **ipv6**—Use IPv6 to check the network connectivity.
- **ipv4-address**—IPv4 address to ping.
- **ipv6-address**—Unicast or Multicast IPv6 address to ping. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. See IPv6z Address Conventions.
- **hostname**—Hostname to ping (Length: 1-160 characters. Maximum label size for each part of the host name: 63.)
- **size *packet_size***—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64–1518, IPv6: 68–1518)
- **count *packet_count***—Number of packets to send, from 1 to 65535 packets. The default is 4 packets. If 0 is entered, it pings until stopped (0–65535).
- **time *time-out***—Timeout in milliseconds to wait for each reply, from 50 to 65535 milliseconds. The default is 2000 milliseconds (50–65535).

Default Usage

N/A

Command Mode

EXEC mode

User Guidelines

Press **Esc** to stop pinging. Following are sample results of the ping command:

- **Destination does not respond**—If the host does not respond, a “no answer from host” appears within 10 seconds.
- **Destination unreachable**—The gateway for this destination indicates that the destination is unreachable.
- **Network or host unreachable**—The switch found no corresponding entry in the route table.

See IPv6z Address Conventions.

When using the ping **ipv6** command to check network connectivity of a directly attached host using its link local address, the egress interface may be specified in the **IPv6Z** format. If the egress interface is not specified, the default interface is selected.

When using the ping **ipv6** command with a Multicast address, the information displayed is taken from all received echo responses.

Examples

Example 1 - Ping an IP address.

```
switchxxxxxx# ping ip 10.1.1.1
Pinging 10.1.1.1 with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

Example 2 - Ping a site.

```
switchxxxxxx# ping ip yahoo.com
Pinging yahoo.com [66.218.71.198] with 64 bytes of data:
64 bytes from 10.1.1.1: icmp_seq=0. time=11 ms
64 bytes from 10.1.1.1: icmp_seq=1. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=2. time=8 ms
64 bytes from 10.1.1.1: icmp_seq=3. time=7 ms
----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 7/8/11
```

Example 3 - Ping an IPv6 address.

```
switchxxxxxx# ping ipv6 3003::11
Pinging 3003::11 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::11: icmp_seq=2. time=50 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
----3003::11 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/12/50
```

```
switchxxxxxx# ping ipv6 FF02::1
Pinging FF02::1 with 64 bytes of data:
64 bytes from 3003::11: icmp_seq=1. time=0 ms
64 bytes from 3003::33: icmp_seq=1. time=70 ms
64 bytes from 3003::11: icmp_seq=2. time=0 ms
64 bytes from 3003::55: icmp_seq=1. time=1050 ms
64 bytes from 3003::33: icmp_seq=2. time=70 ms
```

```
64 bytes from 3003::55: icmp_seq=2. time=1050 ms
64 bytes from 3003::11: icmp_seq=3. time=0 ms
64 bytes from 3003::33: icmp_seq=3. time=70 ms
64 bytes from 3003::11: icmp_seq=4. time=0 ms
64 bytes from 3003::55: icmp_seq=3. time=1050 ms
64 bytes from 3003::33: icmp_seq=4. time=70 ms
64 bytes from 3003::55: icmp_sq=4. time=1050 ms
---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received
```

4.2 traceroute

To display the routes that packets will take when traveling to their destination, use the **traceroute** EXEC mode command.

Syntax

traceroute ip *{ipv4-address | hostname}* ***[size*** *packet_size]* ***[ttl*** *max-ttl]* ***[count*** *packet_count]* ***[timeout*** *time_out]* ***[source*** *ip-address]* ***[tos*** *tos*]

traceroute ipv6 *{ipv6-address | hostname}* ***[size*** *packet_size]* ***[ttl*** *max-ttl]* ***[count*** *packet_count]* ***[timeout*** *time_out]* ***[source*** *ip-address]* ***[tos*** *tos*]

Parameters

- **ip**—Use IPv4 to discover the route.
- **ipv6**—Use IPv6 to discover the route.
- **ipv4-address**—IPv4 address of the destination host.
- **ipv6-address**—IPv6 address of the destination host.
- **hostname**—Hostname of the destination host. (Length: 1-160 characters. Maximum label size for each part of the host name: 63.)
- **size** *packet_size*—Number of bytes in the packet not including the VLAN tag. The default is 64 bytes. (IPv4:64-1518, IPv6: 68-1518)
- **ttl** *max-ttl*—The largest TTL value that can be used. The default is 30. The **traceroute** command terminates when the destination is reached or when this value is reached. (Range: 1–255)
- **count** *packet_count*—The number of probes to be sent at each TTL level. The default count is 3. (Range: 1–10)
- **timeout** *time_out*—The number of seconds to wait for a response to a probe packet. The default is 3 seconds. (Range: 1–60)
- **source** *ip-address*—One of the interface addresses of the device to use as a source address for the probes. The device selects the optimal source address by default. (Range: Valid IP address)
- **tos** *tos*—The Type-Of-Service byte in the IP Header of the packet. (Range: 0–255)

Default Usage

N/A

Command Mode

EXEC mode

User Guidelines

The traceroute command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The traceroute command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The traceroute command sends several probes at each TTL level and displays the round-trip time for each.

The traceroute command sends out one probe at a time. Each outgoing packet can result in one or two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "destination unreachable" error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

The traceroute command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with Esc.

The traceroute command is not relevant to IPv6 link local addresses.

Example

```
switchxxxxxx# traceroute ip umaxp1.physics.lsa.umich.edu
Type Esc to abort.
Tracing the route to umaxp1.physics.lsa.umich.edu (141.211.101.64)
1 i2-gateway.stanford.edu (192.68.191.83)  0 msec 0 msec 0 msec
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (198.32.8.80)   47 msec 45 msec 45 msec
7 so-0-2-0x1.aa1.mich.net (192.122.183.9)  56 msec  53 msec 54 msec
8 atm1-0x24.michnet8.mich.net (198.108.23.82)  56 msec 56 msec 57 msec
9 * * *
10 A-ARB3-LSA-NG.c-SEB.umnet.umich.edu(141.211.5.22)58 msec 58msec 58
msec
11 umaxp1.physics.lsa.umich.edu (141.211.101.64)  62 msec 63 msec 63 msec
Trace completed
```

The following table describes the significant fields shown in the display:

Field	Description
1	Indicates the sequence number of the router in the path to the host.
i2-gateway.stanford.edu	Host name of this router.
192.68.191.83	IP address of this router.
1 msec 1 msec 1 msec	Round-trip time for each of the probes that are sent.

The following are characters that can appear in the traceroute command output:

Field	Description
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
F	Fragmentation required and DF is set.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
R	Fragment reassembly time exceeded
S	Source route failed.
U	Port unreachable.

4.3 telnet

The **telnet** EXEC mode command enables logging on to a host that supports Telnet.

Syntax

telnet {*ip-address* | *hostname*} [*port*] [*keyword*...]

Parameters

- **ip-address**—Specifies the destination host IP address (IPv4 or IPv6).
- **hostname**—Specifies the destination host name. (Length: 1-160 characters. Maximum label size for each part of the host name: 63.)
- **port**—Specifies the decimal TCP port number or one of the keywords listed in the Ports table in the User Guidelines.
- **keyword**—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

Default Configuration

The default port is the Telnet port (23) on the host.

By default, Telnet is disabled.

Command Mode

EXEC mode

User Guidelines

Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To enter a Telnet sequence, press the escape sequence keys (Ctrl-shift-6) followed by a Telnet command character.

Special Telnet Sequences

Telnet Sequence	Purpose
Ctrl-shift-6-b	Break
Ctrl-shift-6-c	Interrupt Process (IP)
Ctrl-shift-6-h	Erase Character (EC)
Ctrl-shift-6-o	Abort Output (AO)
Ctrl-shift-6-t	Are You There? (AYT)
Ctrl-shift-6-u	Erase Line (EL)

At any time during an active Telnet session, available Telnet commands can be listed by pressing the `?/help` keys at the system prompt.

A sample of this list follows.

```
switchxxxxxx# ?/help
[Special telnet escape help]
^^ B sends telnet BREAK
^^ C sends telnet IP
^^ H sends telnet EC
^^ O sends telnet AO
^^ T sends telnet AYT
^^ U sends telnet EL
?/help suspends the session (return to system command prompt)
```

Several concurrent Telnet sessions can be opened, enabling switching between the sessions. To open a subsequent session, the current connection has to be suspended by pressing the escape sequence keys (Ctrl-shift-6) and x to return to the system command prompt. Then open a new connection with the telnet EXEC mode command.

This command lists concurrent Telnet connections to remote hosts that were opened by the current Telnet session to the local device. It does not list Telnet connections to remote hosts that were opened by other Telnet sessions.

Keywords Table

Options	Description
/echo	Enables local echo.
/quiet	Prevents onscreen display of all messages from the software.
/source-interface	Specifies the source interface.
/stream	Turns on stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
Ctrl-shift-6 x	Returns to the System Command Prompt.

Ports Table

Keyword	Description	Port Number
BGP	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web	80

Example
The following example displays logging in to IP address 176.213.10.50 via Telnet.

```
switchxxxxxx# telnet 176.213.10.50
```

4.4 resume
The **resume** EXEC mode command enables switching to another open Telnet session.

Syntax
resume [*connection*]

Parameters
connection—Specifies the connection number. (Range: 1-4 connections.)

Default Configuration
The default connection number is that of the most recent connection.

Command Mode
EXEC mode

Example
The following command switches to open Telnet session number 1.

```
switchxxxxxx# resume 1
```

4.5 hostname
The **hostname** Global Configuration mode command specifies or modifies the device host name. Use the **no** form of the command to remove the existing host name.

Syntax
hostname *name*

no hostname

Parameters
Name—Specifies the device host name. (Length: 1-160 characters. Maximum label size for each part of the host name: 63). The hostname must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens.

Default Configuration
No host name is defined.

Command Mode
Global Configuration mode

Example
The following example specifies the device host name as ‘enterprise’.

```
switchxxxxxx(config)# hostname enterprise
enterprise(config)#
```

4.6 reload
The **reload** Privileged EXEC mode command reloads the operating system.

Syntax
reload [**slot** *unit-id]*

Parameters
slot *unit-id*—Specifies the new master unit number. (Range: 1–8). If unspecified, reloads all the units.

Default Usage
N/A

Command Mode
Privileged EXEC mode

Example
The following example reloads the operating system on all units.

```
switchxxxxxx# reload
This command will reset the whole system and disconnect your current
session. Do you want to continue? (y/n) [Y]
```

4.7 service cpu-utilization
The **service cpu-utilization** Global Configuration mode command enables measuring CPU utilization. Use the **no** form of this command to restore the default configuration.

Syntax
service cpu-utilization

no service cpu-utilization

Parameters
N/A

Default Configuration
Measuring CPU utilization is disabled.

Command Mode
Global Configuration mode

User Guidelines
Use the **service cpu utilization** command to measure information on CPU utilization.

Example
The following example enables measuring CPU utilization.

```
switchxxxxxx(config)# service cpu-utilization
```

4.8 show cpu utilization
The **show cpu utilization** Privileged EXEC mode command displays information about CPU utilization.

Syntax
show cpu utilization

Parameters
N/A

Default Usage
N/A

Command Mode
Privileged EXEC mode

User Guidelines
Use the **show cpu-utilization** command to enable measuring CPU utilization.

Example
The following example displays CPU utilization information.

```
switchxxxxxx# show cpu utilization
CPU utilization service is on.
CPU utilization
-------------------------------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

4.9 clear cpu counters
The **clear cpu counters** EXEC mode command clears traffic counters to and from the CPU.

Syntax
clear cpu counters

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

Example
The following example clears the CPU traffic counters.

```
switchxxxxxx# clear cpu counters
```

4.10 service cpu-counters
The **service cpu-counters** Global Configuration mode command enables traffic counting to and from the CPU. To disable counting, use the **no** form of this command.

Syntax
service cpu-counters

no service cpu-counters

Parameters
N/A

Default Usage
N/A

Command Mode
Global Configuration mode

User Guidelines
Use the **show cpu counters** command to display the CPU traffic counters.

Example
The following example enables counting CPU traffic.

```
switchxxxxxx(config)# service cpu-counters
```

4.11 show cpu counters
The **show cpu counters** EXEC mode command displays traffic counter information to and from the CPU.

Syntax
show cpu counters

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

User Guidelines
Use the **service cpu-counters** command to enable traffic counting to and from the CPU.

Example
The following example displays the CPU traffic counters.

```
switchxxxxxx# show cpu counters
CPU counters are active.
In Octets: 987891
In Unicast Packets: 3589
In Multicast Packets: 29
In Broadcast Packets: 8
Out Octets: 972181
Out Unicast Packets: 3322
Out Multicast Packets: 22
Out Broadcast Packets: 8
```

4.12 show users
The **show users** EXEC mode command displays information about the active users.

Syntax
show users

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

Example
The following example displays information about the active users.

```
switchxxxxxx# show users

Username            Protocol         Location
----------          -----------      ------------
Bob                 Serial
John                SSH              172.16.0.1
Robert              HTTP             172.16.0.8
Betty               Telnet           172.16.1.7
Sam                                  172.16.1.6
```

4.13 show sessions
The **show sessions** EXEC mode command displays open Telnet sessions.

Syntax
show sessions

Parameters
N/A

Default Usage
N/A

Command Mode
EXEC mode

User Guidelines
The **show sessions** command displays Telnet sessions to remote hosts opened by the current Telnet session to the local device. It does not display Telnet sessions to remote hosts opened by other Telnet sessions to the local device.

Example
The following example displays open Telnet sessions.

```
switchxxxxxx# show sessions

Connection   Host            Address      Port    Byte
----------   -------------   ----------   -----   ----
1            Remote router   172.16.1.1   23      89
2            172.16.1.2      172.16.1.2   23      8
```

The following table describes significant fields shown above.

Field	Description
Connection	The connection number.
Host	The remote host to which the device is connected through a Telnet session.
Address	The remote host IP address.
Port	The Telnet TCP port number.
Byte	The number of unread bytes for the user to see on the connection.

4.14 show system

The **show system** EXEC mode command displays system information.

Syntax

show system *unit* *unit-id*

Parameters

unit-id — Specifies the unit number. (Range: 1–8)

Command Mode

EXEC mode

Example

The following example displays the system information.

```
switchxxxxxx# show system unit 2
System Type:                          PowerConnect 5548
System Up Time (days,hour:min:sec):   08,23:03:46
System Contact:
System Name:
System Location:
System MAC Address:                   00:99:88:66:33:33
System Object ID:                     1.3.6.1.4.1.674.10895.3031
Type:                                 PowerConnect 5548
Main Power Supply Status:             OK
Fans Status:                          OK
          Unit Temperature (Celsius) Status
-------------  -------------------   -------------
           2   42                    OK
```

4.15 show version

The **show version** EXEC mode command displays system version information.

Syntax

show version md5 [***unit*** *unit-id*]

Parameters

unit *unit* — Specifies the unit number. (Range: 1–8)

Default Usage

Show version on all units if no unit is specified.

Command Mode

EXEC mode

Example

The following example displays system version information.

```
switchxxxxxx# show version
SW Version      1.1.0.5 ( date  15-Sep-2010 time  10:31:33 )
Boot Version    1.1.0.2 ( date  04-Sep-2010 time  21:51:53 )
HW Version      V01
Unit      SW Version    Boot Version     HW Version
------    -----------   ------------     ----------
1         3.131         2.178            1.0.0
2         3.131         2.178            1.0.0
```

4.16 show version md5

Use the **show version md5** EXEC mode command to display external MD5 digest of firmware.

Syntax

show version md5 [***unit*** *unit-id*]

Parameters

unit *unit*—Unit number. (Range: 1–8)

Default Usage

N/A

Command Mode

EXEC mode

Example

```
switchxxxxxx# show version md5
Unit   Filename      Status        MD5  Digest
----   --------      -------       ---------------------------------
1      image1        Active        23FA000012857D8855AABC7577AB5562
1      image2        Not Active    23FA000012857D8855AABEA7451265456
1      boot                        23FA000012857D8855AABC7577AB8999
2      image1        Not Active    23FA000012857D8855AABC757FE693844
2      image2        Active        23FA000012857D8855AABC7577AB5562
2      boot                        23FA000012857D8855AABC7577AC9999
```

4.17 system resources routing

The **system resources routing** Global Configuration mode command configures the routing table maximum size. Use the **no** form of this command to return to the default size.

Syntax

system resources routing *routes hosts interfaces*

no system resources routing

Parameters

- **routes**—Specifies the maximum number of remote networks in the routing table.
- **hosts**—Specifies the maximum number of directly attached hosts.
- **interfaces**—Specifies the maximum number of IP interfaces.

Default Configuration

Hosts(Alleycat): 10-400, default = 100

Hosts(others): 20-800, default = 200

Routes: 20-128, default = 128

IP Interfaces: 2-32, default = 32

Command Mode

Global Configuration mode

User Guidelines

The settings are effective after reboot.

Example

The following example configures the routing table maximum size.

```
switchxxxxxx# system resources routing 20 23 5
```

4.18 show system resources

The **show system resources routings** EXEC mode command displays system routing resource information.

Syntax
show system resources {*routing* }

Parameters
routing—Displays the number of hosts, routers and IP interfaces that are available.

Command Mode
EXEC mode

Example
The following example displays the system routing resources information. The values in the Current Value column show what resources are currently available. The values in the After Reboot Value column show what resources will be available after reboot as a result of system resources routing command.

```
switchxxxxxx# show system resources routing
Parameters          Current Value         After Reboot Value
--------------      ----------------      ------------------
Hosts:              100
Routes:             32
IP Interfaces:      32
```

The **show system tcam utilization** EXEC mode command displays the Ternary Content Addressable Memory (TCAM) utilization.

Syntax
show system tcam utilization [***unit*** *unit-id*]

Parameters
N/A

Default Usage
N/A

unit-id—Specifies the unit number. (Range: 1–8)

Command Mode
EXEC mode

Example
The following example displays TCAM utilization information.

```
switchxxxxxx#  show system tcam utilization
TCAM utilization: 58%
```

```
System: 75%

Unit    TCAM utilization [%]
----    --------------------
1       58
2       57
```

4.19 show system defaults

Use the **show system defaults** EXEC mode command to display system defaults.

Syntax

show system defaults [*session*]

Parameters

session—Show information for specific session only. Available values are: management, 802.1x, port, fdb, port-mirroring, spanning-tree, vlan, voice-vlan, ip-addressing, network-security and qos-acl.

Command Mode

EXEC mode

Examples

switchxxxxxx# **show system defaults**

The **show system id** EXEC mode command displays the system identity information.

Syntax

show system id [***unit*** *unit-id]*

Parameters

unit *unit-id*—Unit number or all. If unspecified, defaults to all. (Range: 1–8)

Command Mode

EXEC mode

Example

The following example displays the system identity information.

```
switchxxxxxx# show system id
```

5 Stack Commands

5.1 stack master

The **stack master** Global/Interface Configuration mode command forces a stack master selection. Use the **no** form of this command to restore the default configuration.

Syntax

stack master unit *unit-id*

no stack master

Parameters

unit-id—Specifies the new master unit number. (Range: 1–2)

Default Configuration

The default is no forced master.

Command Mode

Global Configuration mode or Interface Configuration mode

User Guidelines

This command has the same affect whether it is run from Global or Interface Configuration mode.

Example

The following example forces the stack master to be unit 2.

```
Console(config)# stack master unit 2
```

5.2 switch renumber

Use the **switch renumber** Global Configuration command to change the unit ID of a specific unit.

Syntax

switch *current-unit-id* ***renumber*** *new-unit-id*

Parameters

- **current-unit-id**—Specify Unit number. (Range: 1–8)
- **new-unit-id**—The new unit number. (Range: 1–8)

Default Usage

N/A

Command Mode

Global Configuration mode

Example
The following renumbers unit 1 to unit 2.

```
console#configure
console(config)# switch 1 renumber 2
```

5.3 show switch
The **show switch** EXEC mode command displays stack status information for the stack or stack member.

Syntax
show switch [*unit-id*]

Parameters
unit-id— Specifies the unit number. (Range: 1–8)

Default Usage
Displays information for all units.

Command Mode
EXEC mode

Example
The following examples display the stack status information for all units on the stack and for the unit specified.

```
console#show switch 1
```

```
Unit  MAC Address        Software    Master    Uplink     Downlink   Status
----  -----------------  ----------  --------  ---------  ---------  -------
1     00:31:06:13:16:11  1.2.0.38    Forced    2          link down  master
2     00:24:05:11:08:49  1.2.0.38    Enabled   1          link down  backup
Topology is Chain
Stack image auto synchronization is enabled
Unit Unit Id After Reset
---- ------------------
 1            0
 2            0
```

```
console#show switch 1
Unit:                   1
MAC address:            00:31:06:13:16:11
Master:                 Forced.
Product:                SG500-28P. Software: 1.2.0.38
Uplink unit:            2 Downlink unit: 0.
Status:                 master
```

```
Active image:           image2.
Selected for next boot: image1.
Topology is Chain
Stack image auto synchronization is enabled
Unit Num After Reset:   0
console#
```

6 Clock Commands

6.1 clock set

The **clock set** Privileged EXEC mode command manually sets the system clock.

Syntax

clock set *hh*:*mm*:*ss* {[*day month*] | [*month day*]} *year*

Parameters

- **hh:mm:ss**—Specifies the current time in hours (military format), minutes, and seconds. (Range: hh: 0-23, mm: 0-59, ss: 0-59)
- **day**—Specifies the current day of the month. (Range: 1-31)
- **month**—Specifies the current month using the first three letters of the month name. (Range: Jan–Dec)
- **year**—Specifies the current year. (Range: 2000–2037)

Command Mode

Privileged EXEC mode

User Guidelines

It is recommended that the user enter the local clock time and date.

Example

The following example sets the system time to 13:32:00 on March 7th, 2005.

```
switchxxxxxx# clock set 13:32:00 7 Mar 2005
```

6.2 clock source

The **clock source** Global Configuration mode command configures an external time source for the system clock. Use the **no** form of this command to disable the external time source.

Syntax

clock source {**sntp**}

no clock source

Parameters

sntp—Specifies that an SNTP server is the external clock source.

Default Configuration

There is no external clock source.

Command Mode

Global Configuration mode

Example

The following example configures an SNTP server as an external time source for the system clock.

```
switchxxxxxx(config)# clock source sntp
```

6.3 clock timezone

Use the **clock timezone** Global Configuration command to set the time zone for display purposes. Use the **no** form of this command to set the time to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same.

Syntax

clock timezone *zone hours-offset [minutes-offset]*

no clock timezone

Parameters

- **zone**—The acronym of the time zone.(Range: Up to 4 characters)
- **hours-offset**—Hours difference from UTC. (Range: (-12)–(+13))
- **minutes-offset**—Minutes difference from UTC. (Range: 0–59)

Default Configuration

Offsets are **0**.

Acronym is empty.

Command Mode

Global Configuration mode

User Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

Example

```
switchxxxxxx(config)# clock timezone abc +2 minutes 32
```

6.4 clock summer-time

Use one of the formats of the **clock summer-time** Global Configuration command to configure the system to automatically switch to summer time (Daylight Saving Time). Use the **no** form of this command to configure the software not to automatically switch to summer time.

Syntax

clock summer-time *zone* ***recurring*** *{**usa** | **eu** | {week day month hh:mm week day month hh:mm}} [offset]*

clock summer-time *zone* ***date*** *day month year hh:mm date month year hh:mm [offset]*

clock summer-time *zone* ***date*** *month day year hh:mm month day year hh:mm [offset]*

no clock summer-time

Parameters

- **zone**—The acronym of the time zone to be displayed when summer time is in effect. (Range: up to 4 characters)
- **recurring**—Indicates that summer time starts and ends on the corresponding specified days every year.
- **date**—Indicates that summer time starts on the first date listed in the command and ends on the second date in the command.
- **usa**—The summer time rules are the United States rules.
- **eu**—The summer time rules are the European Union rules.
- **week**—Week of the month. Can be 1–4, first, last.
- **day**—Day of the week (first three characters by name, such as Sun).
- **date**—Date of the month. (Range: 1–31)
- **month**—Month (first three characters by name, such as Feb).
- **year**—year (no abbreviation). (Range: 2000–2097)
- **hh:mm**—Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- **offset**—Number of minutes to add during summer time (default is 60). (Range: 1440)

Default Configuration

Summer time is disabled.

Command Mode

Global Configuration mode

User Guidelines

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

USA rules for Daylight Saving Time:

- From 2007:
  - Start: Second Sunday in March
  - End: First Sunday in November
  - Time: 2 AM local time
- Before 2007:
  - Start: First Sunday in April
  - End: Last Sunday in October
  - Time: 2 AM local time

EU rules for Daylight Saving Time:

- Start: Last Sunday in March
- End: Last Sunday in October
- Time: 1.00 am (01:00) Greenwich Mean Time (GMT)

Example

```
switchxxxxxx(config)# clock summer-time abc date apr 1 2010 09:00 aug 2
2010 09:00
```

6.5 clock dhcp timezone

Use the **clock dhcp timezone** Global Configuration command to specify that the timezone and the Summer Time (Daylight Saving Time) of the system can be taken from the DHCP Timezone option. Use the **no** form of this command disable this option.

Syntax

clock dhcp timezone

no clock dhcp timezone

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The TimeZone taken from the DHCP server has precedence over the static TimeZone. If the TimeZone does not exist in the DHCP-TimeZone option, the static configuration will be active.

The Summer Time taken from the DHCP server has precedence over static SummerTime. If the Summer Time does not exist in the DHCP-TimeZone option, the static configuration will be active.

The TimeZone and SummerTime remain effective after the IP address lease time has expired.

The TimeZone and SummerTime that are taken from the DHCP server are cleared after reboot.

When the user disables taking the TimeZone and Summer Time from the DHCP server, the dynamic Time Zone and Summer Time from the DHCP server are cleared.

In case of multiple DHCP-enabled interfaces, the last accepted DHCP-Time Zone option overrides any previous DHCP-Time Zone option. This means that the last accepted DHCP-Time Zone option overrides the previous Time Zone and the Summer Time, even if it includes only one of them.

Disabling the DHCP client from where the DHCP-TimeZone option was taken, clears the dynamic Time Zone and Summer Time configuration.

Example

```
switchxxxxxx(config)# clock dhcp timezone
```

6.6 sntp authentication-key

The **sntp authentication-key** Global Configuration mode command defines an authentication key for Simple Network Time Protocol (SNTP). Use the **no** form of this command to remove the authentication key for SNTP.

Syntax

sntp authentication-key *key-number* **md5** *key-value*

no sntp authentication-key *key-number*

Parameters

- **key-number**—Specifies the key number. (Range: 1–4294967295)
- **md5** *key-value*—Specifies the key value. (Length: 1–8 characters)

Default Configuration

No authentication key is defined.

Command Mode

Global Configuration mode

Examples

The following example defines the authentication key for SNTP.

```
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate
```

6.7 sntp authenticate

The **sntp authenticate** Global Configuration mode command enables authentication for received SNTP traffic from servers. Use the **no** form of this command to disable the feature.

Syntax

sntp authenticate

no sntp authenticate

Parameters

N/A

Default Configuration

Authentication is disabled.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both Unicast and Broadcast.

Examples

The following example enables authentication for received SNTP traffic and sets the key and encryption key.

```
switchxxxxxx(config)# sntp authenticate
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
```

6.8 sntp trusted-key

The **sntp trusted-key** Global Configuration mode command authenticates the identity of the system with which SNTP synchronizes. Use the **no** form of this command to disable system identity authentication.

Syntax

sntp trusted-key *key-number*

no sntp trusted-key *key-number*

Parameters

key-number—Specifies the key number of the authentication key to be trusted. (Range: 1–4294967295)

Default Configuration

No keys are trusted.

Command Mode

Global Configuration mode

User Guidelines

The command is relevant for both received unicast and broadcast.

Examples

The following example authenticates key 8.

```
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authentication-key 8 md5 ClkKey
switchxxxxxx(config)# sntp trusted-key 8
switchxxxxxx(config)# sntp authenticate
```

6.9 sntp client poll timer

The **sntp client poll timer** Global Configuration mode command sets the polling time for the SNTP client. Use the no form of this command to restore the default configuration.

Syntax

sntp client poll timer *seconds*

no sntp client poll timer

Parameters

seconds—Specifies the polling interval in seconds. (Range: 60–86400)

Default Configuration

The default polling interval is 1024 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the polling time for the SNTP client to 120 seconds.

```
switchxxxxxx(config)# sntp client poll timer 120
```

6.10 sntp broadcast client enable

The **sntp broadcast client enable** Global Configuration mode command enables SNTP Broadcast clients. Use the no form of this command to disable SNTP Broadcast clients.

Syntax

sntp broadcast client enable

no sntp broadcast client enable

Default Configuration

The SNTP Broadcast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp broadcast client enable** Interface Configuration mode command to enable the SNTP Broadcast client on a specific interface.

After entering this command, you must enter clock source snmp for the command to be run. If this command is not run, the switch will not synchronize with Broadcast servers.

Example

The following example enables SNTP Broadcast clients.

```
switchxxxxxx(config)# sntp broadcast client enable
```

6.11 sntp anycast client enable

The **sntp anycast client enable** Global Configuration mode command enables the SNTP Anycast client. Use the **no** form of this command to disable the SNTP Anycast client.

Syntax

sntp anycast client enable

no sntp anycast client enable

Parameters

N/A

Default Configuration

The SNTP anycast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enable the SNTP Anycast client.

Example

The following example enables SNTP Anycast clients.

```
switchxxxxxx(config)# sntp anycast client enable
```

6.12 sntp client enable

The **sntp client enable** Global Configuration mode command enables the SNTP Broadcast and Anycast client on an interface when the device is in Router mode (Layer 3). Use the **no** form of this command to disable the SNTP Broadcast and Anycast client.

Syntax

sntp client enable {*interface-id*}

no sntp client enable {*interface-id*}

Parameters

interface-id—Specifies an interface ID, which can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Global Configuration mode - Ethernet port, Port-channel or VLAN.

User Guidelines

This command only works when the device is in Router mode (Layer 3).

The sntp broadcast client enable Global Configuration mode command globally enables Broadcast clients.

The sntp anycast client enable Global Configuration mode command globally enables Anycast clients.

This command enables both.

Example

The following example enables the SNTP Broadcast and Anycast client on port fe1/0/13.

```
switchxxxxxx(config)# sntp client enable fe1/0/13
```

6.13 sntp unicast client enable

The **sntp unicast client enable** Global Configuration mode command enables the device to use Simple Network Time Protocol (SNTP)-predefined Unicast clients. Use the **no** form of this command to disable the SNTP Unicast clients.

Syntax

sntp unicast client enable

no sntp unicast client enable

Parameters

N/A

Default Configuration

The SNTP unicast client is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the sntp server Global Configuration mode command to define SNTP servers.

Example

The following example enables the device to use SNTP Unicast clients.

```
switchxxxxxx(config)# sntp unicast client enable
```

6.14 sntp unicast client poll

The **sntp unicast client poll** Global Configuration mode command enables polling for the SNTP predefined Unicast clients. Use the **no** form of this command to disable the polling for the SNTP client.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Configuration

Polling is disabled.

Command Mode

Global Configuration mode

User Guidelines

Polling time is configured with the **sntp client poll timer** Global Configuration mode command.

Example

The following example enables polling for SNTP predefined unicast clients.

```
switchxxxxxx(config)# sntp unicast client poll
```

6.15 sntp server

The **sntp server** Global Configuration mode command configures the device to use the SNTP to request and accept Network Time Protocol (NTP) traffic from a specified server (meaning to accept system time from an SNTP server). Use the **no** form of this command to remove a server from the list of SNTP servers.

Syntax

sntp server {*ip-address* | *hostname*} [***poll***] [***key*** *keyid*]

no sntp server {*ip-address* | *hostname*}

Parameters

- **ip-address**—Specifies the server IP address. This can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions:
- **hostname**—Specifies the server hostname. Only translation to IPv4 addresses is supported. (Length: 1–158 characters. Maximum label length for each part of the hostname: 63 characters)
- **poll**—Enables polling.
- **key** *keyid*—Specifies the Authentication key to use when sending packets to this peer. (Range:1–4294967295)

Default Configuration

No servers are defined.

Command Mode

Global Configuration mode

User Guidelines

Up to 8 SNTP servers can be defined.

The sntp unicast client enable Global Configuration mode command enables predefined Unicast clients.

The sntp unicast client poll Global Configuration mode command globally enables polling.

Polling time is configured with the sntp client poll timer Global Configuration mode command.

Example

The following example configures the device to accept SNTP traffic from the server on 192.1.1.1 with polling.

```
switchxxxxxx(config)# sntp server 192.1.1.1 poll
```

6.16 sntp port

The **sntp port** Global Configuration mode command specifies a SNTP User Datagram Protocol (UDP) port. Use the **no** form of this command to use the SNTP server default port.

Syntax

sntp port *port-number*

no sntp port

Parameters

port-number—Specifies the UDP port number used by an SNTP server. (Range 1–65535)

Default Configuration

The default port number is 123.

Command Mode

Global Configuration mode

Example

The following example specifies that port 321 of the SNTP server is the UDP port.

```
switchxxxxxx(config)# sntp port 321
```

6.17 show clock

The **show clock** EXEC mode command displays the time and date from the system clock.

Syntax

show clock [*detail*]

Parameters

detail—Displays the time zone and summer time configuration.

Command Mode

EXEC mode

Examples

Example 1 - The following example displays the system time and date.

```
switchxxxxxx# show clock
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP
```

Example 2 - The following example displays the system time and date along with the time zone and summer time configuration.

```
switchxxxxxx# show clock detail
15:29:03 PDT(UTC-7) Jun 17 2002
Time source is SNTP
Time zone:
Acronym is PST
Offset is UTC-8
Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
Ends at last Sunday of October at 2:00.
Offset is 60 minutes.
DHCP timezone: Disabled
```

6.18 show sntp configuration

The **show sntp configuration** Privileged EXEC mode command displays the SNTP configuration on the device.

Syntax

show sntp configuration

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the device's current SNTP configuration.

```
switchxxxxxx# show sntp configuration
SNTP port : 123 .
```

```
Polling interval: 1024 seconds.
No MD5 authentication keys.
Authentication is not required for synchronization.
No trusted keys.

Unicast Clients: Enabled
Unicast Clients Polling: Enabled
Server       Polling   Encryption Key
------------ -------   --------------
1.1.1.121    Disabled     Disabled
Broadcast Clients: disabled
Anycast Clients: disabled
No Broadcast Interfaces.
switchxxxxxx#
```

6.19 show sntp status

The **show sntp status** Privileged EXEC mode command displays the SNTP servers status.

Syntax

show sntp status

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the SNTP servers status.

```
switchxxxxxx# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8, unicast
Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:
Server         Status       Last response               Offset     Delay
                                                        [mSec]     [mSec]
----------     -------      ---------------------       ------     ------
176.1.1.8      Up           19:58:22.289 PDT Feb 19     7.33       117.79
                            2005
176.1.8.179    Unknown      12:17.17.987 PDT Feb 19     8.98       189.19
                            2005
```

```
Anycast server:
Server          Interface     Status     Last response      Offset      Delay
----------      ---------     ------     ------------       [mSec]      [mSec]
176.1.11.8      VLAN 118      Up         9:53:21.789 PDT    ------      ------
                                         Feb 19 2005        7.19        119.89

Broadcast:
Server          Interface                Last response
---------       ---------                -----------------
176.9.1.1       VLAN 119                 19:17:59.792
                                         PDT Feb 19 2002
```

7 Auto-Update and Auto-Configuration

7.1 boot host auto-config

Use the **boot host auto-config** Global Configuration mode command to enable auto configuration via DHCP. Use the **no** form of this command to disable DHCP auto configuration.

Syntax

boot host auto-config

no boot host auto-config

Parameters

N/A

Default Configuration

Enabled by default.

Command Mode

Global Configuration mode

Default Configuration

Enabled by default.

Example

```
switchxxxxxx(conf)# boot host auto-config
```

7.2 boot host auto-update

Use the **boot host auto-update** Global Configuration mode command to enable the support of auto updated via DHCP. Use the **no** form of this command to disable DHCP auto configuration.

Syntax

boot host auto-update

no boot host auto-update

Parameters

N/A

Default Configuration

Enabled by default.

Command Mode

Global Configuration mode

Default Configuration
Enabled by default.

Example

```
switchxxxxxx(conf)# boot host auto-update
```

7.3 boot host dhcp
Use the **boot host dhcp** Global Configuration mode command to force downloading a configuration file at the next system startup. Use the **no** form of this command to restore the host configuration file to the default.

Syntax
boot host dhcp

no boot host dhcp

Parameters
N/A

Default Configuration
Disabled.

Command Mode
Global Configuration mode

User Guidelines
Configuring **boot host dhcp** does not take effect until the next reboot.

7.4 boot host auto-save
Use the **boot host auto-save** Global Configuration mode command to automatically save the Running configuration file in the Startup configuration file after download. Use the **no** form of this command restore default behavior.

Syntax
boot host auto-save

no boot host auto-save

Parameters
N/A

Default Configuration
Disable

Command Mode
Global Configuration mode

Examples

```
switchxxxxxx(conf)# boot host auto-save
```

7.5 show boot

Use the **show boot** Privilege EXEC mode command to show the status of the IP DHCP Auto Config process.

Syntax

show boot

Parameters

N/A

Default Configuration

N/A

Command Mode

Privilege EXEC mode

Examples

```
switchxxxxxx show boot



 Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: force
Auto Config State: Finished
TFTP Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg
      Auto Update
      -----------
Image Download via DHCP: enabled
```

```
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Opening <hostname>-config file
```

```
            Auto Update
            -------------
Image Download via DHCP: enabled
```

```
Example 3.
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Downloading configuration file
Auto Update
-----------
Image Download via DHCP: enabled
```

```
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Searching hostname in indirect configuration file
Auto Update
-----------
Image Download via DHCP: enabled
```

```
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Quit - failed all steps of finding existing configuration file
Auto Update
-----------
Image Download via DHCP: enabled
```

```
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Update
```

```
-----------
Image Download via DHCP: enabled
Auto Update State: Downloaded indirect image file
```

```
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Update
-----------
Image Download via DHCP: enabled
Auto Update State: Downloading image file
```

```
switchxxxxxx# show boot
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: default
Auto Config State: Finished
TFTP Server IP address: 1.2.20.2
Configuration filename: /config/configfile1.cfg
Auto Update
-----------
Image Download via DHCP: enabled
Auto Update State: Downloading image file
```

7.6 ip dhcp tftp-server ip address

Use the **ip dhcp tftp-server ip address** Global Configuration mode command to set the TFTP server's IP address. This address server as the default address used by a switch when it has not been received from the DHCP server.

Use the **no** form of this command to remove the address.

Syntax

ip dhcp tftp-server ip address *ip-addr*

no ip dhcp tftp-server ip address

Parameters

ip addr *ip-addr*—Address of TFTP server

Default Configuration

No IP address

Command Mode
Global Configuration mode

Examples

```
switchxxxxxx(conf)# ip dhcp tftp-server ip address 10.5.234.232
```

7.7 ip dhcp tftp-server file

Use the **ip dhcp tftp-server file** Global Configuration mode command to set the full file name of the configuration file to be downloaded on the TFTP server when it has not been received from the DHCP server. This serves as the default configuration file.

Use the **no** form of this command to remove the name.

Syntax
ip dhcp tftp-server file *file-path*

no ip dhcp tftp-server file

Parameters
file-path—Full file path and name of the configuration file on TFTP server

Default Configuration
No file name

Command Mode
Global Configuration mode

Examples

```
switchxxxxxx(conf)# ip dhcp tftp-server file conf/conf-file
```

7.8 show ip dhcp tftp-server

Use the **show ip dhcp tftp-server** EXEC mode command to display information about the TFTP server.

Syntax
show ip dhcp tftp-server

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC

Example

```
switchxxxxxx# show ip dhcp tftp server
tftp server address
active     1.1.1.1 from sname
manual     2.2.2.2
file path on tftp server
active     conf/conf-file from option 67
```

8 Configuration and Image File Commands

8.1 copy

The **copy** Privileged EXEC mode command copies a source file to a destination file.

Syntax

copy *source-url destination-url* ***[snmp]***

Parameters

- **source-url**—Specifies the source file URL or source file reserved keyword to be copied. (Length: 1–160 characters)
- **destination-url**—Specifies the destination file URL or destination file reserved keyword. (Length: 1–160 characters).
- **snmp**—Specifies that the destination/source file is in SNMP format. Used only when copying from/to the Startup Configuration file.

The following table displays the URL options.

Keyword	Source or Destination
flash://	Source or destination URL for flash memory. This is the default URL If a URL is specified without a prefix.
running-config	Currently running configuration file.
startup-config	Startup configuration file.
image	Image file. If specified as the source file, it is the active image file. If specified as the destination file, it is the non-active image file.
boot	Boot file.
tftp://	Source or destination URL for a TFTP network server. The syntax for this alias is *tftp://host/[directory]/filename*. The host can be either an IP address or a host name.
xmodem:	Source for the file from a serial connection that uses the Xmodem protocol.
unit:*//member/***image**	Image file on one of the units. To copy from the master to all units, specify * in the member field.
unit:*//member/***boot**	Boot file on one of the units. To copy from the master to all units, specify * in the member field
unit:*//member/* **startup-config**	Configuration file used during initialization (startup) on one of the units.
null:	Null destination for copies or files. A remote file can be copied to null to determine its size. For instance **copy running-conf null** returns the size of the running configuration file.
backup-config	Backup configuration file. A configuration file can be downloaded to this file (without giving a file name). This can then be copied to the running-conf or startup-conf files.
unit://*member*/**backup-config**	Backup configuration file on one of the units.

Keyword	Source or Destination
mirror-config	Mirrored configuration file. If the running config and the startup config have been identical for 24 hours, the startup config is automatically copied to the mirror-conf file by the system. It can then be copied to the startup or running conf if required.
ogging	Specifies the SYSLOG file.
Word<1-128>	Name of file.

Command Mode

Privileged EXEC mode

User Guidelines

The location of the file system dictates the format of the source or destination URL.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

IPv6z Address Format

If the IPv6 address is a Link Local address (IPv6z address), the outgoing interface name must be specified. The format of an IPv6z address is: {*ipv6-link-local-address*}**%**{*interface-id*}. The subparameters are:

- **ipv6-link-local-address**—Specifies the IPv6 Link Local address.
- **interface-id**—{<port-type>[ ]<port-number>}|{port-channel | po}[]<port-channel-number> | {tunnel | tu}[ ]<tunnel-number> | vlan[ ]<vlan-id>

If the egress interface is not specified, the default interface is selected. The following combinations are possible:

- **ipv6_address%interface_id** - Refers to the IPv6 address on the interface specified.
- **ipv6_address%0 -** Refers to the IPv6 address on the single interface on which an IPv6 address is defined.
- **ipv6_address -** Refers to the IPv6 address on the single interface on which an IPv6 address is defined.

Invalid Combinations of Source and Destination

The following are invalid combinations of source and destination files:

- The source file and destination file are the same file.
- **xmodem:** is the destination file. The source file can be copied to **image**, **boot** and **null:** only.
- **tftp://** is the source file and destination file on the same copy.
- ***.prv** files cannot be copied. The source or destination is a slave unit (except for image and boot files).
- **mirror-config** cannot be used as a destination

The following table describes the characters displayed by the system when **copy** is being run:

Character	Description
!	For network transfers, indicates that the copy process is taking place. Each exclamation point indicates successful transfer of ten packets (512 bytes each).
.	For network transfers, indicates that the copy process timed out.

Various Copy Options Guidelines

- **Copying an Image File from a Server to Flash Memory**
  Use the **copy** *source-url* **flash://image** command to copy an image file from a server to flash memory. When the administrator copies an image file from the server to a device, the image file is saved to the "inactive" image. To use this image, the administrator must switch the inactive image to the active image and reboot. The device will then use this new image.
- **Copying a Boot File from a Server to Flash Memory**
- Use the **copy** *source-url* **boot** command to copy a boot file from a server to flash memory.
  Copying a Configuration File from a Server to the Running Configuration File
  Use the **copy** *source-url* **running-config** command to load a configuration file from a network server to the running configuration file of the device. The commands in the loaded configuration file are added to those in the running configuration file as if the commands were typed in the command-line interface (CLI). The resulting configuration file is a combination of the previous running configuration and the loaded configuration files, with the loaded configuration file taking precedence.
- **Copying a Configuration File from a Server to the Startup Configuration**
  Use the **copy** *source-url* **startup-config** command to copy a configuration file from a network server to the device startup configuration file. The startup configuration file is replaced by the copied configuration file.
- **Storing the Running Config or Startup Config on a Server**
  Use the **copy running-config** *destination-url* command to copy the current configuration file to a network server using TFTP.
  Use the **copy startup-config** *destination-url* command to copy the startup configuration file to a network server.
- **Saving the Running Configuration to the Startup Configuration**
  Use the **copy running-config startup-config** command to copy the running configuration to the startup configuration file.
- -**Backing Up the Running Configuration or Startup Configuration to a Backup Configuration file**
  Use the **copy running-config flash://***file_name* command to back up the running configuration to a backup configuration file.
  Use the **copy startup-config flash://***file_name* command to back up the startup configuration to a backup configuration file.
- **Backing Up the Running Configuration or Startup Configuration to the Backup Configuration**
  Use the **copy running-config backup-config** command to back up the running configuration to the backup configuration file.
  Use the **copy startup-config backup-config** command to back up the startup configuration to the backup configuration file.
- **Restoring the Mirror Configuration File.**
  Use **copy mirror-config startup-config** or **copy mirror-config running-config** to copy the mirror configuration file to one of the configuration files being used.

Examples

Example 1 - The following example copies system image file1 from the TFTP server 172.16.101.101 to the non-active image file.

```
switchxxxxxx# copy tftp://172.16.101.101/file1 image
```

```
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Example 2 - Copying an Image from a Server to Flash Memory

The following example copies a system image named file1 from the TFTP server with an IP address of 172.16.101.101 to a non-active image file.

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://image
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! [OK]
Copy took 0:01:11 [hh:mm:ss]
```

Example 3 - Copying the mirror-config file to the startup-configuration file

The following example copies the mirror configuration file, saved by the system, to the Startup Configuration file.

```
switchxxxxxx# copy mirror-config startup-config
```

8.2 write memory

Use the **write memory** Privileged EXEC mode command to save the Running Configuration file to the Startup Configuration file.

Syntax

write memory

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

This example shows how to overwrite the startup-config with the running-config.

```
switchxxxxxx# write memory
Overwrite file [startup-config] ?[Yes/press any key for no]....15-Sep-2010
11:27
:48 %COPY-I-FILECPY: Files Copy - source URL running-config destination
URL flash://startup-config
15-Sep-2010 11:27:50 %COPY-N-TRAP: The copy operation was completed
successfully
Copy succeeded
```

8.3 delete

The **delete** Privileged EXEC mode command deletes a file from a flash memory device.

Syntax

delete *url*

Parameters

url—Specifies the location URL or reserved keyword of the file to be deleted. (Length: 1–160 characters)

The following table displays keywords and URL prefixes:

Keyword	Source or Destination
flash://	URL of the flash memory. This is the default URL if a URL is specified without a prefix.
startup-config	Startup configuration file.
WORD	Name of file.

Default Configuration
N/A

Command Mode
Privileged EXEC mode

User Guidelines
***.sys**, ***.prv**, **image-1** and **image-2** files cannot be deleted.

Example
The following example deletes the file called ‘test’ from the flash memory.

```
switchxxxxxx# delete flash://test
Delete flash:test? [confirm]
```

8.4 pwd
Use the **pwd** Privileged EXEC mode command to display a full, clarified path to the current directory.

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example deletes the file called ‘test’ from the flash memory.

```
switchxxxxxx# pwd
```

8.5 dir
The **dir** Privileged EXEC mode command displays the list of files on a flash file system.

Syntax
dir *[directory-path]*

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the list of files on a flash file system

```
Total size of flash: 33292288 bytes
Free size of flash: 20708893 bytes
switchxxxxxx# dir
Directory of flash:
File Name   Permission  Flash Size Data Size    Modified
---------   ----------  ---------- ---------    ---------
tmp         rw          524288     104          01-Jan-2010 05:35:04
image-1     rw          10485760   10485760     01-Jan-2010 06:10:23
image-2     rw          10485760   10485760     01-Jan-2010 05:43:54
dhcpsn.prv  --          262144     --           01-Jan-2010 05:25:07
sshkeys.prv    --       262144      --           04-Jan-2010 06:05:00
syslog1.sys    r-       524288      --           01-Jan-2010 05:57:00
syslog2.sys    r-       524288      --           01-Jan-2010 05:57:00
directry.prv   --       262144      --           01-Jan-2010 05:25:07
startup-config rw       786432     1081          01-Jan-2010 10:05:34
Total size of flash: 66322432 bytes
Free size of flash: 42205184 bytes
```

8.6 more
The **more** Privileged EXEC mode command displays a file.

Syntax
more *url*

Parameters
url—Specifies the location URL or reserved keyword of the source file to be displayed. (Length: 1–160 characters).

The following table displays options for the URL parameter:

Keyword	Source or Destination
flash://	Source or destination URL for flash memory. If a URL is specified without a prefix, this is the default URL.
running-config	Current running configuration file.
startup-config	Startup configuration file.
mirror-config	Mirrored configuration file.

Default Configuration
N/A

Command Mode
Privileged EXEC mode

User Guidelines
Files are displayed in ASCII format, except for the images, which are displayed in a hexadecimal format.

***.prv** files cannot be displayed.

Example
The following example displays the running configuration file contents.

```
switchxxxxxx# more running-config
no spanning-tree
interface range fe1/0/11-48
speed 1000
exit
no lldp run
line console
exec-timeout 0
```

8.7 cd

Use the **cd** Privileged EXEC mode command to change the current directory, for example from flash to usb.

cd *new-directory*

Parameters
new-directory—The new directory. The new directory path may be specified as either a Full Clarified Path or a Relative Path.

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

User Guidelines
When command **cd** changes the current file system, the current directory of the previous file system is saved and when the command specifying only the file system (for example, **cd**:) sets the file system as current, the current directory is restored.

Example

```
console cd ://private/conf
console pwd
switchxxxxxx# cd flash:
console pwd
flash://
console cd :
console pwd
switchxxxxxx# cd flash://
console pwd
flash:\\
console cd ://
console pwd
```

8.8 rename

The **rename** Privileged EXEC mode command renames a file.

Syntax

rename *url new-url*

Parameters

- **url**—Specifies the file location URL. (Length: 1–160 characters)
- **new-url**—Specifies the file's new URL. (Length: 1–160 characters)

The following table displays options for the URL parameter:

Keyword	Source or Destination
flash://	URL for flash memory. If a URL is specified without a prefix, this is the default URL.
WORD<1-128>	Name of file.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

***.sys** and ***.prv** files cannot be renamed.

Example

The following example renames the configuration backup file.

```
switchxxxxxx# rename configuration.bak m-config.bak
```

8.9 boot system

The **boot system** Privileged EXEC mode command specifies the active system image file that will be loaded by the device at startup.

Syntax

boot system ***{image-1*** | ***image-2} [switch*** *unit-id* | ***all]***

Parameters

- **switch** *unit-id***—**Specifies the unit number. If unspecified, defaults to the master unit number.
- **all—**Specifies that the active image of all units is being set by the command.
- **image-1**—Specifies that image-1 is loaded as the system image during the next device startup.
- **image-2**—Specifies that image-2 is loaded as the system image during the next device startup.

Default Configuration

The default unit number is the master unit number.

Command Mode

Privileged EXEC mode

User Guidelines

Use the show bootvar command to display the active image.

Example

The following example specifies that **image-1** is the active system image file loaded by the device at startup. The results of this command is displayed in show bootvar.

```
switchxxxxxx# boot system image-1
switchxxxxxx#show bootvar
Unit   Image   Filename    Version     Date                      Status
----   -----   ---------   ---------   ---------------------     -----------
1      1       image-1     1.2.0.34    04-Jul-2011  15:03:07     Not active*
1      2       image-2     1.2.0.38    13-Jul-2011  17:51:53     Active
2      1       image-1     1.2.0.38    13-Jul-2011  17:51:53     Active*
2      2       image-2     1.2.0.34    04-Jul-2011  15:03:07     Not active
"*" designates that the image was selected for the next boot
```

8.10 show running-config

Use the **show running-config** privileged EXEC command to display the contents of the currently running configuration file.

Syntax

show running-config

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the running configuration file contents.

```
switchxxxxxx# show running-config
no spanning-tree
interface range fe1/0/11-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#
```

8.11 show startup-config

Use the **show startup-config** Privileged EXEC mode command to display the Startup Configuration file contents.

Syntax
show startup-config

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the startup configuration file contents.

```
switchxxxxxx# show startup-config
no spanning-tree
interface range fe1/0/11-48
speed 1000
exit
no lldp run
interface vlan 1
ip address 1.1.1.1 255.0.0.0
exit
line console
exec-timeout 0
exit
switchxxxxxx#
```

8.12 show backup-config

Use the **show backup-config** Privileged EXEC mode command to display the Backup Configuration file contents.

Syntax

show backup-config

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the Backup Configuration file contents.

```
switchxxxxxx# show backup-config
software version 1.1
hostname device
interface fe1/0/11
ip address 176.242.100.100 255.255.255.0
duplex full
speed 1000
interface fe1/0/12
ip address 176.243.100.100 255.255.255.0
duplex full
speed 1000
```

8.13 show bootvar

Use the **show bootvar** EXEC mode command to display the active system image file that is loaded by the device at startup.

Syntax

show bootvar ***[unit** unit-id]*

Parameters

unit-id—Specifies the unit number. Range 1-8

Command Mode

EXEC mode

Example

The following example displays the active system image file that is loaded by the device at startup.

```
switchxxxxxx# show bootvar

Unit      Image        filename      Version      Date              Status
----      -----        --------      -------      --------------    -----------
1         1            file1         3.1.31       23-Jul-2002       Active
1         2            file2         3.2.19       22-Jan-2003       Not active*
2         1            file1         3.1.31       23-Jul-2002       Not active
2         2            file2         3.2.19       22-Jan-2003  2    Active

"*": Designates that the image was selected for the next boot.
```

9 Management ACL Commands

9.1 management access-list

The **management access-list** Global Configuration mode command configures a management access list (ACL) and enters the Management Access-List Configuration command mode. Use the **no** form of this command to delete an ACL

Syntax

management access-list *name*

no management access-list *name*

Parameters

name—Specifies the ACL name. (Length: 1–32 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure a management access list. This command enters the Management Access-List Configuration mode, where the denied or permitted access conditions are defined with the **deny** and **permit** commands.

If no match criteria are defined, the default value is **deny**.

When re-entering the access-list context, the new rules are entered at the end of the access list.

Use the management access-class command to select the active access list.

The active management list cannot be updated or removed.

For IPv6 management traffic that is tunneled in IPv4 packets, the management ACL is applied first on the external IPv4 header (rules with the service field are ignored), and then again on the inner IPv6 header.

Example

Example 1 - The following example creates a management access list called **mlist**, configures management `fe1/0/1`1 and `fe1/0/1`9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit fe1/0/11
switchxxxxxx(config-macl)# permit fe1/0/19
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)# management access-class mlist
```

Example 2 - The following example creates a management access list called ‘mlist’, configures all interfaces to be management interfaces except `fe1/0/11 and 9`, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny fe1/0/11
switchxxxxxx(config-macl)# deny fe1/0/19
switchxxxxxx(config-macl)# permit
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)# management access-class mlist
```

9.2 permit (Management)

The **permit** Management Access-List Configuration mode command sets permit rules (ACEs) for the management access list (ACL).

Syntax

permit *[interface-id] [service service]*

permit ip-source {*ipv4-address* | *ipv6-address*/*ipv6-prefix-length*} ***[mask*** *{mask* | *prefix-length}] [interface-id] [**service** service]*

Parameters

- **interface-id**:—Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service* — Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address**— Specifies the source IPv4 address.
- **ipv6-address/ipv6-prefix-length**— Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (/). The parameter is optional.
- **mask** *mask* — Specifies the source IPv4 address network mask. This parameter is relevant only to IPv4 addresses.
- **mask** *prefix-length* — Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (/). This parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration

No rules are configured.

Command Mode

Management Access-List Configuration mode

User Guidelines

Rules with Ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example
The following example permits all ports in the ACL called **mlist**

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit
```

9.3 deny (Management)
The **deny** Management Access-List Configuration mode command sets permit rules (ACEs) for the management access list (ACL).

Syntax
deny *[interface-id] [**service** service]*

deny ip-source *{ipv4-address | ipv6-address/ipv6-prefix-length} [**mask** {mask | prefix-length}] [interface-id] [**service** service]*

Parameters
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service*—Specifies the service type. Possible values are: Telnet, SSH, HTTP, HTTPS and SNMP.
- **ipv4-address**—Specifies the source IPv4 address.
- **ipv6-address/ipv6-prefix-length**—Specifies the source IPv6 address and source IPv6 address prefix length. The prefix length must be preceded by a forward slash (*/*). The parameter is optional.
- **mask** *mask*—Specifies the source IPv4 address network mask. The parameter is relevant only to IPv4 addresses.
- **mask** *prefix-length*—Specifies the number of bits that comprise the source IPv4 address prefix. The prefix length must be preceded by a forward slash (*/*). The parameter is relevant only to IPv4 addresses. (Range: 0–32)

Default Configuration
No rules are configured.

Command Mode
Management Access-List Configuration mode

User Guidelines
Rules with ethernet, VLAN, and port-channel parameters are valid only if an IP address is defined on the appropriate interface.

Example
The following example denies all ports in the ACL called **mlist**.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny
```

9.4 management access-class

The **management access-class** Global Configuration mode command restricts management connections by defining the active management access list (ACL). To disable management connection restrictions, use the **no** form of this command.

Syntax

management access-class {**-only** | *name*}

no management access-class

Parameters

- **-only**—Specifies that the device can be managed only from the .
- **name**—Specifies the ACL name to be used. (Length: 1–32 characters)

Default Configuration

The default configuration is no management connection restrictions.

Command Mode

Global Configuration mode

Example

The following example defines an access list called **mlist** as the active management access list.

```
switchxxxxxx(config)# management access-class mlist
```

9.5 show management access-list

The **show management access-list** Privileged EXEC mode command displays management access lists (ACLs).

Syntax

show management access-list [*name*]

Parameters

name—Specifies the name of a management access list to be displayed. (Length: 1–32 characters)

Default Configuration

All management ACLs are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the **mlist** management ACL.

```
switchxxxxxx# show management access-list mlist
```

```
-only
------------
deny
! (Note: all other access implicitly denied)
mlist
-----
permit fe1/0/11
permit fe1/0/19
! (Note: all other access implicitly denied)
switchxxxxxx#
```

9.6 show management access-class

The **show management access-class** Privileged EXEC mode command displays information about the active management access list (ACLs).

Syntax

show management access-class

Command Mode

Privileged EXEC mode

Example

The following example displays the active management ACL information.

```
switchxxxxxx# show management access-class
Management access-class is enabled, using access list mlist
```

10 Network Management Protocol (SNMP) Commands

10.1 snmp-server community

Use the **snmp-server community** Global Configuration mode command to set the community access string (password) that permits access to SNMP commands (v1 and v2). This is used for SNMP commands, such as GETs and SETs.

This command configures both SNMP v1 and v2.

Use the **no** form of this command to remove the specified community string.

Syntax

snmp-server community *community-string [**ro** | **rw** | **su**]* [*ip-address* | *ipv6-address*] *[**mask** mask* | **prefix** *prefix-length] [**view** view-name]*

snmp-server community-group *community-string group-name [ip-address* | *ipv6-address] [**mask** mask* | **prefix** *prefix-length]*

no snmp-server community *community-string [ip-address]*

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters). This string is used as an input parameter to snmp-server user for SNMP v3.
- **ro**—Specifies read-only access (default)
- **rw**—Specifies read-write access
- **su**—Specifies SNMP administrator access
- **view** *view-name*—Specifies the name of a view configured using the command snmp-server view (no specific order of the command configurations is imposed on the user). The view defines the objects available to the community. It is not relevant for **su**, which has access to the whole MIB. If unspecified, all the objects, except the community-table and SNMPv3 user and access tables, are available. (Range: 1–30 characters)
- **ip-address**—Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **mask**—Specifies the mask of the IPv4 address. This is not a network mask, but rather a mask that defines which bits of the packet's source address are compared to the configured IP address. If unspecified, it defaults to 255.255.255.255. The command returns an error if the mask is specified without an IPv4 address.
- **prefix-length**—Specifies the number of bits that comprise the IPv4 address prefix. If unspecified, it defaults to 32. The command returns an error if the prefix-length is specified without an IPv4 address.
- **group-name**—This is the name of a group configured using snmp-server group with v1 or v2 (no specific order of the two command configurations is imposed on the user). The group defines the objects available to the community. (Range: 1–30 characters)

Default Configuration

No community is defined

Command Mode
Global Configuration mode

User Guidelines
Use **snmp-server community-group** to configure access rights to a user group. The group must exist in order to be able to specify the access rights. Otherwise, the community-group will not be useful.

A *view-name* cannot be specified for **su**, which has access to the whole MIB tree.

The logical key of the command is the pair (community, ip-address). If ip-address is omitted then the key is (community, All-IPs). This means that there cannot be two commands with the same community, ip address pair.

The *view-name* is used to restrict the access rights of a community string. When a view-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to an internal group-name.
- Maps the internal group-name for SNMPv1 and SNMPv2 security models to view-name (read-view and notify-view always, and for rw for write-view also),

The *group-name* is used to restrict the access rights of a community string. When a group-name is specified, the software:

- Generates an internal security-name.
- Maps the internal security-name for SNMPv1 and SNMPv2 security models to the group-name.

Examples
Example 1 - Defines a password for administrator access to the management station at IP address 1.1.1.121 and mask 255.0.0.0.

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask
255.0.0.0
```

Example 2 - Defines a password *tom* for the group *abcd* that enables this group to access the management station 1.1.1.121 with prefix 8.

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122
prefix 8
```

10.2 snmp-server view
The **snmp-server view** Global Configuration mode command creates or updates an SNMP view. Use the **no** form of this command to remove an SNMP view.

Syntax
snmp-server view *view-name oid-tree* {***included*** | ***excluded***}

no snmp-server view *view-name* [*oid-tree*]

Parameters
- **view-name**—Specifies the name for the view that is being created or updated. (Length: 1–30 characters)

- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System and, optionally, a sequence of numbers. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4. This parameter depends on the MIB being specified.
- **included**—Specifies that the view type is included.
- **excluded**—Specifies that the view type is excluded.

Default Configuration
The following views are created by default:

- **Default** - Contains all MIBs except for those that configure the SNMP parameters themselves.
- **DefaultSuper** - Contains all MIBs.

Command Mode
Global Configuration mode

User Guidelines
This command can be entered multiple times for the same view.

The command's logical key is the pair (view-name, oid-tree). Therefore there cannot be two commands with the same view-name and oid-tree.

The number of views is limited to 64.

Default and DefaultSuper views are reserved for internal software use and cannot be deleted or modified.

Example
The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interface group (this format is specified on the parameters specified in ifEntry).

```
switchxxxxxx(config)# snmp-server view user-view system included
switchxxxxxx(config)# snmp-server view user-view system.7 excluded
switchxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

10.3 show snmp views
Use the **show snmp views** Privileged EXEC mode command to display the SNMP views.

Syntax
show snmp views [*viewname*]

Parameters
viewname—Specifies the view name. (Length: 1–30 characters)

Default Configuration
If viewname is not specified, all views are displayed.

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP views.

```
switchxxxxxx# show snmp views

Name                 OID Tree                      Type
----------------     ----------------------        ----------
Default              iso                           Included
Default              snmpNotificationMIB           Excluded
DefaultSuper         iso                           Included
```

10.4 snmp-server group

Use the **snmp-server group** Global Configuration mode command to configure an SNMP group. Groups are used to map SNMP users to SNMP views (using snmp-server user). Use the **no** form of this command to remove an SNMP group.

Syntax
snmp-server group *groupname* {***v1*** | ***v2*** | ***v3*** *{**noauth*** | ***auth*** | ***priv**}* *[**notify** notifyview]}* *[**read** readview]* *[**write** writeview]*

no snmp-server group *groupname {**v1*** | ***v2*** | ***v3** [**noauth*** | ***auth*** | ***priv**]}*

Parameters
- **group** *groupname*—Specifies the group name. (Length: 1–30 characters)
- **v1**—Specifies the SNMP Version 1 security model.
- **v2**—Specifies the SNMP Version 2 security model.
- **v3**—Specifies the SNMP Version 3 security model.
- **noauth**—Specifies that no packet authentication will be performed. Applicable only to the SNMP version 3 security model.
- **auth**—Specifies that packet authentication without encryption will be performed. Applicable only to the SNMP version 3 security model.
- **priv**—Specifies that packet authentication with encryption will be performed. Applicable only to the SNMP version 3 security model. Note that creation of SNMPv3 users with both authentication and privacy must be done in the GUI. All other users may be created in the CLI.
- **notify** *notifyview*—Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgement. Applicable only to the SNMP version 3 security model. (Length: 1–30 characters)
- **read** *readview*—Specifies the view name that enables viewing only. (Length: 1–30 characters)
- **write** *writeview*—Specifies the view name that enables configuring the agent. (Length: 1–30 characters)

Default Configuration
No group entry exists.

If *notifyview* is not specified, the notify view is not defined.

If *readview* is not specified, all objects except for the community-table and SNMPv3 user and access tables are available for retrieval.

If *writeview* is not specified, the write view is not defined.

Command Mode
Global Configuration mode

User Guidelines
The group defined in this command is used in snmp-server user to map users to the group. These users are then automatically mapped to the views defined in this command.

The command logical key is (**groupname, snmp-version, security-level**). For snmp-version v1/v2 the security-level is always **noauth**.

Example
The following example attaches a group called *user-group* to SNMPv3, assigns the encrypted security level to the group, and limits the access rights of a view called *user-view* to read-only. User *tom* is then assigned to *user-group*. So that user *tom* has the rights assigned in *user-view*.

```
switchxxxxxx(config)# snmp-server group user-group v3 priv read
user-view
switchxxxxxx(config)# snmp-server user tom user-group v3
```

10.5 show snmp groups
Use the **show snmp groups** Privileged EXEC mode command to display the configured SNMP groups.

Syntax
show snmp groups [*groupname*]

Parameters
groupname—Specifies the group name. (Length: 1–30 characters)

Default Configuration
Display all groups.

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP groups.

```
switchxxxxxx# show snmp groups
```

```
Name                    Security                Views

                Model     Level       Read      Write     Notify
-------------   -----     ----        -------   -------   -------
user-group      V3        priv        Default   ""        ""
managers-group  V3        priv        Default   Default   ""
```

The following table describes significant fields shown above.

Field		Description
Name		Group name.
Security	Model	SNMP model in use (v1, v2 or v3).
Security	Level	Packet authentication with encryption. Applicable to SNMP v3 security only.
Views	Read	View name enabling viewing the agent contents. If unspecified, all objects except the community-table and SNMPv3 user and access tables are available.
	Write	View name enabling data entry and managing the agent contents.
	Notify	View name enabling specifying an inform or a trap.

10.6 snmp-server user

Use the **snmp-server user** Global Configuration mode command to configure a new SNMP Version user. Use the **no** form of the command to remove a user.

Syntax

snmp-server user *username groupname {**v1** | **v2c** | [**remote** host] **v3**[**encrypted**] [**auth** { **md5** | **sha**} auth-password]}*

no snmp-server user *username [**remote** host]*

Parameters

- **username**—Define the name of the user on the host that connects to the agent. (Range: Up to 20 characters). For SNMP v1 or v2c, this username must match the community string entered in snmp-server host.
- **groupname**—The name of the group to which the user belongs. The group should be configured using the command snmp-server group with v1 or v2c parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- **remote** *host*—IPaddress (IPv4, IPv6 or IPv6z) or host name of the remote SNMP host. See IPv6z Address Conventions.
- **v1**—Specifies that the user is a v1 user.
- **v2c**—Specifies that the user is a v2c user..
- **v3**—Specifies that the user is a v3 user..
- **encrypted**—Specifies whether the password that follows appears in encrypted format. If it is in encrypted format, it servers as the key.
- **auth**—Specifies which authentication level is to be used.
- **md5**—Specifies the HMAC-MD5-96 authentication level.

- **Sha**—Specifies the HMAC-SHA-96 authentication level.

auth-password—Specifies the authentication password. Range: Up to 32 characters.**Default Configuration**
No group entry exists.

Command Mode
Global configuration

User Guidelines
For SNMP v1 and v2, this performs the same actions as **snmp-server community-group**, except that **snmp-server community-group** configures both v1 and v2 at the same time. With this command, you must perform it once for v1 and once for v2.

When you enter a **show running-config** command, you do not see a line for this SNMP user. To see if this user has been added to the configuration, type the **show snmp user** command.

An SNMP EngineID must be defined in order to add SNMPv3 users to the device (in the snmp-server engineID local or snmp-server engineID remote commands).

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users' database.

The logical key of the command is username.

Configuring a remote host is required in order to send informs to that host, because an inform is a trap that requires acknowledgement.. A configured remote host is also able to manage the device (besides getting the informs)

To configure a remote user, specify the IP address for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the snmp-server engineID remote command. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command fails.

Since the same group may be defined several times, each time with different version or different access level (noauth, auth or auth & priv), when defining a user it is not sufficient to specify the group name, rather you must specify group name, version and access level for complete determination of how to handle packets from this user.

Example
This example assigns user *tom* to group *abcd* using SNMP v1 and v2c. The default is assigned as the engineID. User *tom* is assigned to group *abcd* using SNMP v1 and v2c

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user tom acbd v3
```

10.7 show snmp users
Use the **show snmp users** Privileged EXEC mode command to display the configured SNMP users.

Syntax
show snmp users [*username*]

Parameters
username—Specifies the user name. (Length: 1–30 characters)

Default Configuration
Display all users.

Command Mode
Privileged EXEC mode

Example
The following example displays the configured SNMP users.

```
switchxxxxxx# show snmp users

                        Auth
Name      Group name    Method     Remote
-------   -----------   -------    ----------------------
John      user-group    md5
John      user-group    md5        08009009020C0B099C07-5879
```

10.8 snmp-server filter
The **snmp-server filter** Global Configuration mode command creates or updates an SNMP server notification filter. Use the **no** form of this command to remove a notification filter.

Syntax
snmp-server filter *filter-name oid-tree {**included** | **excluded**}*

no snmp-server filter *filter-name* [*oid-tree*]

Parameters
- **filter-name**—Specifies the label for the filter record that is being updated or created. The name is used to reference the filter in other commands. (Length: 1–30 characters)
- **oid-tree**—Specifies the ASN.1 subtree object identifier to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as System. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example, 1.3.*.4.
- **included**—Specifies that the filter type is included.
- **excluded**—Specifies that the filter type is excluded.

Default Configuration
No view entry exists.

Command Mode
Global Configuration mode

User Guidelines

This command can be entered multiple times for the same filter. If an object identifier is included in two or more lines, later lines take precedence.The command's logical key is the pair (filter-name, oid-tree).

Example

The following example creates a filter that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group (this format depends on the parameters define din ifEntry).

```
switchxxxxxx(config)# snmp-server filter f1 system included
switchxxxxxx(config)# snmp-server filter f2 system.7 excluded
switchxxxxxx(config)# snmp-server filter f3 ifEntry.*.1 included
```

10.9 show snmp filters

Use the **show snmp filters** Privileged EXEC mode command to display the defined SNMP filters.

Syntax

show snmp filters [*filtername*]

Parameters

filtername—Specifies the filter name. (Length: 1–30 characters)

Default Configuration

If filtername is not defined, all filters are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays the configured SNMP filters.

```
switchxxxxxx# show snmp filters user-filter
Name             OID Tree                    Type
-----------      --------------------        ---------
user-filter      1.3.6.1.2.1.1               Included
user-filter      1.3.6.1.2.1.1.7             Excluded
user-filter      1.3.6.1.2.1.2.2.1.*.1       Included
```

10.10 snmp-server host

Use the **snmp-server host** Global Configuration mode command to configure the host for SNMP notifications: (traps/informs). Use the **no** form of this command to remove the specified host.

Syntax

snmp-server host *{host-ip | hostname}* ***[traps | informs] [version*** *{1 | 2c | 3* ***[auth | noauth | priv]}]*** *community-string* ***[udp-port*** *port]* ***[filter*** *filtername]* ***[timeout*** *seconds]* ***[retries*** *retries]*

no snmp-server host *{ip-address | hostname}* ***[traps | informs] [version*** *{****1*** *|* ***2c*** *|* ***3}]***

Parameters

- **host-ip**—IP address of the host (the targeted recipient). The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **hostname**—Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- **trap**—Sends SNMP traps to this host (default).
- **informs**—Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.
- **1**—SNMPv1 traps are used.
- **2c**—SNMPv2 traps or informs are used
- **3**—SNMPv2 traps or informs are used
- **community-string**—Password-like community string sent with the notification operation. (Range: 1–20 characters). For v1 and v2, any community string can be entered here. For v3, the community string must match the user name defined in snmp-server user for v3.
- Authentication options are available for SNMP v3 only. The following options are available:
  - **noauth**—Specifies no authentication of a packet.
  - **auth**—Specifies authentication of a packet without encryption.
  - **priv**—Specifies authentication of a packet with encryption.
- **udp-port** *port*—UDP port of the host to use. The default is 162. (Range: 1–65535)
- **filter** *filtername*—Filter for this host. If unspecified, nothing is filtered. The filter is defined using snmp-server filter (no specific order of commands is imposed on the user). (Range: Up to 30 characters)
- **timeout** *seconds*—(For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)
- **retries** *retries*—(For informs only) Maximum number of times to resend an inform request, when a response is not received for a generated message. The default is 3. (Range: 0–255)

Default Configuration

Version: SNMP V1

Type of notification: Traps

udp-port: 162

If informs are specified, the default for retries: 3

Timeout: 15

Command Mode

Global Configuration mode

User Guidelines

The logical key of the command is the pair (ip-address/hostname, traps/informs, version).

When configuring SNMP v1 or v2 notifications recipient, the software automatically generates a notification view for that recipient for all MIBs.

For SNMPv3 the software does not automatically create a user or a notify view.

Use the commands snmp-server user, snmp-server group and snmp-server view to create a user, a group or a notification group, respectively.

Example

The following defines a host at the IP address displayed.

```
switchxxxxxx(config)# snmp-server host 1.1.1.121 abc
```

10.11 snmp-server engineID local

The **snmp-server engineID local** Global Configuration mode command specifies the SNMP engineID on the local device for SNMP v3. Use the **no** form of this command to remove this engine ID.

Syntax

snmp-server engineID local {*engineid-string* | ***default***}

no snmp-server engineID local

Parameters

- **engineid-string**—Specifies a concatenated hexadecimal character string identifying the engine ID. Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. If an odd number of hexadecimal digits are entered, the system automatically prefixes the digit 0 to the string. (Length: 5–32 characters, 9–64 hexadecimal digits)
- **default**—Specifies that the engine ID is created automatically based on the device MAC address.

Default Configuration

The default engine ID is defined per standard as:

- First 4 octets: First bit = 1, the rest is IANA Enterprise number = 674.
- Fifth octet: Set to 3 to indicate the MAC address that follows.
- Last 6 octets: The device MAC address.

Command Mode

Global Configuration mode

User Guidelines

To use SNMPv3, an engine ID must be specified for the device. Any ID can be specified or the default string, which is generated using the device MAC address, can be used.

As the engineID should be unique within an administrative domain, the following guidelines are recommended:

- For standalone devices, use the default keyword to configure the Engine ID.
- For stackable systems, configure an EngineID, and verify that it is unique within the administrative domain.

Changing or removing the value of **snmpEngineID** deletes the SNMPv3 users database.

The SNMP EngineID cannot be all 0x0 or all 0xF or 0x000000001

Example

The following example enables SNMPv3 on the device and sets the device local engine ID to the default value.

```
switchxxxxxx(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
Do you wish to continue? [Y/N]Y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y
```

10.12 snmp-server engineID remote

To specify the SNMP engine ID of a remote SNMP device, use the **snmp-server engineID remote** Global Configuration mode command. Use the **no** form of this command to remove the configured engine ID.

Syntax

snmp-server engineID remote *{ip-address} engineid-string*

no snmp-server engineID remote *{ip-address}*

Parameters

- **ip-address** —IPv4, IPv6 or IPv6z address of the remote device. See IPv6z Address Conventions.
- **engineid-string**—The character string that identifies the engine ID. The engine ID is a concatenated hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. If the user enters an odd number of hexadecimal digits, the system automatically prefixes the hexadecimal string with a zero. (Range: engineid-string5–32 characters. 9–64 hexadecimal digits)

Default Configuration

The remote engineID is not configured by default.

Command Mode

Global Configuration mode

User Guidelines

A remote engine ID is required when an SNMP version 3 inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

10.13 show snmp engineID

Use the **show snmp engineID** Privileged EXEC mode command to display the local SNMP engine ID.

Syntax

show snmp engineID

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the SNMP engine ID.

```
switchxxxxxx # show snmp engineID
Local SNMP engineID: 08009009020C0B099C075878
IP address     Remote SNMP engineID
-----------    ------------------------------
172.16.1.1     08009009020C0B099C075879
```

10.14 snmp-server enable traps

Use the **snmp-server enable traps** Global Configuration mode command to enable the device to send all SNMP traps. Use the **no** form of the command to disable all SNMP traps.

Syntax
snmp-server enable traps

no snmp-server enable traps

Default Configuration
SNMP traps are enabled.

Command Mode
Global Configuration mode

User Guidelines
If **no snmp-server enable traps** has been entered, you can enable failure traps by using snmp-server trap authentication as shown in the example.

Example
The following example enables SNMP traps except for SNMP failure traps.

```
switchxxxxxx(config)# snmp-server enable traps
switchxxxxxx(config)# no snmp-server trap authentication
```

10.15 snmp-server trap authentication

Use the **snmp-server trap authentication** Global Configuration mode command to enable the device to send SNMP traps when authentication fails. Use the **no** form of this command to disable SNMP failed authentication traps.

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Parameters

N/A

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

User Guidelines

The command snmp-server enable traps enables all traps including failure traps. Therefore, if that command is enabled (it is enabled by default), this command is not necessary.

Example

The following example disables all SNMP traps and enables only failed authentication traps.

```
switchxxxxxx(config)# no snmp-server enable traps
switchxxxxxx(config)# snmp-server trap authentication
```

10.16 snmp-server contact

Use the **snmp-server contact** Global Configuration mode command to set the value of the system contact (sysContact) string. Use the **no** form of the command to remove the system contact information.

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

text—Specifies system contact information. (Length: 1–168 characters)

Default Configuration

N/A

Command Mode

Global Configuration mode

Example
The following example sets the system contact information to Technical_Support.

```
switchxxxxxx(config)# snmp-server contact Technical_Support
```

10.17 snmp-server location
Use the **snmp-server location** Global Configuration mode command to set the value of the system location string. Use the **no** form of this command to remove the location string.

Syntax
snmp-server location *text*

no snmp-server location

Parameters
text—Specifies the system location information. (Length: 1–160 characters)

Default Configuration
N/A

Command Mode
Global Configuration mode

Example
The following example sets the device location to New_York.

```
switchxxxxxx(config)# snmp-server location New_York
```

10.18 snmp-server set
Use the **snmp-server set** Global Configuration mode command to define SNMP MIB commands in the configuration file if a MIB performs an action for which there is no corresponding CLI command.

Syntax
snmp-server set *variable-name name value* [*name2 value2*...]

Parameters
- **variable-name**—Specifies an SNMP MIB variable name, which must be a valid string.
- **name** *value*—Specifies a list of names and value pairs. Each name and value must be a valid string. In the case of scalar MIBs, there is only a single name-value pair. In the case of an entry in a table, there is at least one name-value pair, followed by one or more fields.

Default Configuration
N/A

Command Mode
Global Configuration mode

User Guidelines
Although the CLI can set any required configuration, there might be a situation where an SNMP user sets a MIB variable that does not have an equivalent CLI command. To generate configuration files that support those situations, the system uses snmp-server set. This command is not intended for the end user.

Example
The following example configures the scalar MIB sysName with the value TechSupp.

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```

10.19 show snmp
Use the **show snmp** Privileged EXEC mode command to display the SNMP status.

Syntax
show snmp

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the SNMP communications status.

```
switchxxxxxx# show snmp
SNMP is enabled

Community-String     Community-Access      View name          IP Address          Mask
----------------     ----------------      ------------       ----------          ----
public               read only             user-view          All
private              read write            Default            172.16.1.1/10
private              su                    DefaultSuper       172.16.1.1

Community-string     Group name            IP Address         Mask       Type
----------------     ----------            ----------                    ------
public               user-group            All                           Router

Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications
```

```
Target Address       Type      Community    Version     UDP      Filter     TO       Retries
                                                        Port     Name       Sec
-----------          ----      --------     -------     ----     ------     ---      -------
192.122.173.42       Trap      public       2           162                 15       3
192.122.173.42       Inform    public       2           162                 15       3
Version 3 notifications
Target Address       Type      Username     Security    UDP      Filter     TO       Retries
                                            Level       Port     name       Sec
-----------          ----      --------     -------     ----     -----      ---      -------
192.122.173.42       Inform    Bob          Priv        162                 15       3
System Contact: Robert
System Location: Marketing
```

The following table describes the significant fields shown in the display.

Field	Description
Community-string	The community access string permitting access to SNMP.
Community-access	The permitted access type—read-only, read-write, super access.
IP Address	The management station IP Address.
Target Address	The IP address of the targeted recipient.
Version	The SNMP version for the sent trap.

11 RSA and Certificate Commands

11.1 crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates a public and private DSA key (DSA key pair).

Syntax
crypto key generate dsa

Parameters
N/A

Default Configuration
DSA key pairs do not exist.

Command Mode
Global Configuration mode

User Guidelines
DSA keys are generated in pairs - one public DSA key and one private DSA key.

If the device already has DSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the Running configuration file. However, the keys generated by this command are saved in a private configuration (which is never displayed to the user or backed up to another device).

Example
The following example generates a DSA key pair.

```
switchxxxxxx(config)# crypto key generate dsa
The SSH service is generating a private DSA key.
This may take a few minutes, depending on the key size.
.....
```

11.2 crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs.

Syntax
crypto key generate rsa

Parameters
N/A

Default Configuration
RSA key paris do not exist.

Command Mode
Global Configuration mode

User Guidelines
RSA keys are generated in pairs - one public RSA key and one private RSA key.

If the device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys.

This command is not saved in the Running configuration file; however, the keys generated by this command are saved in a private configuration (which is never displayed to the user or backed up to another device).

Example
The following example generates RSA key pairs where a RSA key already exists.

```
switchxxxxxx(config)# crypto key generate rsa
Replace Existing RSA Key [y/n]? N
switchxxxxxx(config)#
```

11.3 show crypto key mypubkey
The **show crypto key mypubkey** Privileged EXEC mode command displays the device's SSH public keys.

Syntax
show crypto key mypubkey *[rsa* | *dsa]*

Parameters
- **rsa**—Displays the RSA key.
- **dsa**—Displays the DSA key.

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the SSH public RSA keys on the device.

```
switchxxxxxx# show crypto key mypubkey dsa
 dsa key data:
ssh-dss AAAAB3NzaC1kc3MAAACBAOY/PhBgItVP5tFgDS7PA6Sdsvg5zq6c
k0VoWb0Pckj5mXy86jPrUdCAFsdwHubfDVr1qJUSz+0e5LfQtu2Sf9mUoyRG
```

```
DeC8PYRurARrP0t9OFNYk+PZazJRjgy/X4V+9YL2etj+OrYm3f3YqLESlzJS
6IIycU1fEGNcZXL5JqM7AAAAFQD3UDWQ/9dXAGhFWy+u1sEqv/6b4wAAAIAs
jjSG4hq0RFdK5ooMKfB8lHAIOF8pI1maywkaoMvJcukzBJ0x+K7DQiRLYQ+r
mrc5rOCs+ZWK8n6qK6Nvlli36mrc5uNM/C/ZcT/T3xu5TpHoujgByaxR+EKA
HSg4lIJagCQjM6TlnhDyLQYpsKdV1yovpSavjhM/gHcGjnwUKwAAAIEAp4RE
oR9ylQwtdiZHQcNXZhkN8eyfV1mirxLfnGiQhX48FdHGLLEQcZZBUFSkTvGr
Te0y3nh2mZwnmKKeu49B6oEFGGVIr/Df2u1igxidHKTdhNqcpMjClZKk3roz
DI7/i4KHlRpaSByY4P7906k/QLDA6vcELMfUw1XH6FwNuNY=
Fingerprint(hex): e5:2e:39:43:e6:a3:3b:8a:9d:c7:62:9f:fc:c6:86:d1
Fingerprint(bubbleBabble):
xesit-mupyd-kihod-cuzem-cigot-zogyr-gafyn-vileg-kunen
-felac-kuxyx
```

11.4 crypto certificate generate

The **crypto certificate generate** Global Configuration mode command generates a self-signed certificate for HTTPS.

Syntax

crypto certificate *number* **generate** ***[key-generate*** *[length]]* ***[passphrase*** *string]* ***[cn*** *common-name]* ***[ou*** *organization-unit]* ***[or*** *organization]* ***[loc*** *location]* ***[st*** *state]* ***[cu*** *country]* ***[duration*** *days*]

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **key-generate** *length*—Regenerates SSL RSA key and specifies the SSL's RSA key length. (Range: 512–2048)
- **passphrase** *string*—Specifies the passphrase used for exporting the certificate in PKCS12 file format. (Length: 8–96 characters)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
  - **cn** *common- name*—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
  - **ou** *organization-unit*—Specifies the organization-unit or department name. (Length: 1–64 characters)
  - **or** *organization*—Specifies the organization name. (Length: 1–64 characters)
  - **loc** *location*—Specifies the location or city name. (Length: 1–64 characters)
  - **st** *state*—Specifies the state or province name. (Length: 1–64 characters)
  - **cu** *country*—Specifies the country name. (Length: 2 characters)
- **duration** *days*—Specifies the number of days a certification is valid. (Range: 30–3650)

Default Configuration

The default SSL's RSA key length is 1024.

If **passphrase** *string* is not specified, the certificate is not exportable.

If **cn** *common- name* is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

If **duration** *days* is not specified, it defaults to 365 days.

Command Mode
Global Configuration mode

User Guidelines
This command is not saved in the Running configuration file. However, the certificate and keys generated by this command are saved in a private configuration (which is never displayed to the user or backed up to another device).

When exporting a RSA key pair to a PKCS#12 file, the RSA key pair is as secure as the passphrase. Keep the passphrase secure.

If the RSA key does not exist, you must use the parameter **key-generate**.

If both certificates 1 and 2 have been generated, use ip https certificate to active one of them.

Example
The following example generates a self-signed certificate for HTTPS whose length is 100 bytes.

```
switchxxxxxx# crypto certificate generate key-generate 100
```

11.5 crypto certificate request
The **crypto certificate request** Privileged EXEC mode command generates and displays a certificate request for HTTPS.

Syntax
crypto certificate *number* **request** *[**cn** common- name] [**ou** organization-unit] [**or** organization] [**loc** location] [**st** state] [**cu** country]*

Parameters
- **number**—Specifies the certificate number. (Range: 1–2)
- The following elements can be associated with the key. When the key is displayed, they are also displayed.
  - **cn** *common- name*—Specifies the fully qualified device URL or IP address. (Length: 1–64 characters). If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
  - **ou** *organization-unit*—Specifies the organization-unit or department name. (Length: 1–64 characters)
  - **or** *organization*—Specifies the organization name. (Length: 1–64 characters)
  - **loc** *location*—Specifies the location or city name. (Length: 1–64 characters)
  - **st** *state*—Specifies the state or province name. (Length: 1–64 characters)
  - **cu** *country*—Specifies the country name. (Length: 2 characters)

Default Configuration
If **cn common-name** is not specified, it defaults to the device's lowest static IPv6 address (when the certificate is generated), or to the device's lowest static IPv4 address if there is no static IPv6 address, or to 0.0.0.0 if there is no static IP address.

Command Mode
Privileged EXEC mode

User Guidelines
Use this command to export a certificate request to a Certification Authority. The certificate request is generated in Base64-encoded X.509 format.

Before generating a certificate request, first generate a self-signed certificate using the crypto certificate generateGlobal Configuration mode command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the crypto certificate import Global Configuration mode command to import the certificate into the device. This certificate replaces the self-signed certificate.

Example
The following example displays the certificate request for HTTPS.

```
switchxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
CN= router.gm.com
0= General Motors
C= US
```

11.6 crypto certificate import
The **crypto certificate import** Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS.

Syntax
crypto certificate *number* **import**

Parameters
number—Specifies the certificate number. (Range: 1–2)

Default Configuration
N/A

Command Mode
Global Configuration mode

User Guidelines
To end the session (return to the command line to enter the next command), enter a blank line.

The imported certificate must be based on a certificate request created by the crypto certificate request privileged EXEC command.

If the public key found in the certificate does not match the device's SSL RSA key, the command fails.

This command is not saved in the Running configuration file. However, the certificate imported by this command is saved in the private configuration (which is never displayed to the user or backed up to another device).

Example
The following example imports a certificate signed by the Certification Authority for HTTPS.

```
switchxxxxxx(config)#exit
switchxxxxxx#crypto certificate
  <1-2>               Specifies the certificate number.
switchxxxxxx#crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE REQUEST-----
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the
input,and press Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
.
```

```
-----END CERTIFICATE-----
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

11.7 crypto certificate export pkcs12

The **crypto certificate export pkcs12** Privileged EXEC mode command exports the certificate and the RSA keys within a PKCS12 file.

Syntax

crypto certificate *number* **export pkcs12**

Parameters

number—Specifies the certificate number. (Range: 1–2)

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This command creates a PKCS 12 file that contains the certificate and an RSA key pair. This is used by crypto certificate import pkcs12.

The passphrase for the export is determined when the key is generated.

The certificate and key pair are exported in a standard PEM-format PKCS12 file. This format can be converted to and from the binary PFX file used by Windows and Linux by using the **openssl** command-line tool. See an open source OpenSSL user manual (man pkcs12) for more information.

Example

The following example exports the certificate and the RSA keys within a PKCS12 file.

```
switchxxxxxx# crypto certificate 1 export pkcs12
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAgTASAxCjAIBgNVBAcTASAxCjAIBgNVBAMTASAxCjAIBgNVBAoTASAxCjAIBgNV
BAsTASAwHhcNMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBJMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMBIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
```

```
ChMBIDEKMAgGA1UECxMBIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIes/sRJE8uahTBJqKu1VHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLeN1p1kARxI4C1fTU
efig3ffZ/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxW/1P0kqSxuMhc25OdBE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpCTb090rx+cNwVfIvjoedgQ
Mtl5+fKIAcqsfEgEGJNXQ4jEzsXAkwfQLFfgt47O3IpkUn0AxrQzutJDOcC28Uxp
raMVTVSlSkJIvaPuXJxdZ279tDMwZffILBfKCJGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYERh7+7JXLKHpd
ueeu3znfIX4dDeti8B3xYvvE8kGZjxFN1cC3zc3JsD0IVu1LkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZXylFzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----
```

11.8 crypto certificate import pkcs12

The **crypto certificate import pkcs12** Privileged EXEC mode command imports the certificate and the RSA keys within a PKCS12 file.

Syntax

crypto certificate *number* **import pkcs12** *passphrase*

Parameters

- **number**—Specifies the certificate number. (Range: 1–2)
- **passphrase**—Specifies the passphrase used to encrypt the PKCS12 file for export. (Length: 8–96 characters)

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This command enables using the passphrase that was exported by crypto certificate export pkcs12. This passphrase must be saved for later exports.

Example

The following example imports the certificate and the RSA keys within a PKCS12 file.

```
switchxxxxxx# crypto certificate 1 import pkcs12 encrypted_passphrase
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
subject=/C=us/ST= /L= /CN= /O= /OU=
issuer= /C=us/ST= /L= /CN= /O= /OU=
-----BEGIN CERTIFICATE-----
MIIBfDCCASYCAQAwDQYJKoZIhvcNAQEEBQAwSTELMAkGA1UEBhMCdXMxCjAIBgNV
BAgTASAxCjAIBgNVBAcTASAxCjAIBgNVBAMTASAxCjAIBgNVBAoTASAxCjAIBgNV
BAsTASAwHhcNMDQwMjA3MTU1NDQ4WhcNMDUwMjA2MTU1NDQ4WjBJMQswCQYDVQQG
EwJ1czEKMAgGA1UECBMBIDEKMAgGA1UEBxMBIDEKMAgGA1UEAxMBIDEKMAgGA1UE
ChMBIDEKMAgGA1UECxMBIDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZXP/tk3e/
jrulfZw8q8T2oS5ymrEIes/sRJE8uahTBJqKu1VHqRYJR3VYa/03HSJ741w5MzPI
iuWZzrbbuXAxAgMBAAEwDQYJKoZIhvcNAQEEBQADQQBQ+GTLeN1p1kARxI4C1fTU
efig3ffZ/tjW5q1t1r5F6zNv/GuXWw7rGzmRyoMXDcYp1TaA4gAIFQCpFGqiSbAx
-----END CERTIFICATE-----
Bag Attributes
localKeyID: 0C 75 81 77 5A 31 53 D1 FF 4E 26 BE 8D 4A FD 8B 22 9F 45 D4
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,085DCBF3A41D2669
dac0m9jqEp1DM50sIDb8Jq1jxW/1P0kqSxuMhc25OdBE/1fPBg9VSvV1ARaYt16W
bX67UyJ8t7HHF3AowjcWzElQ5GJgSQ0VemsqsRQzjpCTb090rx+cNwVfIvjoedgQ
Mtl5+fKIAcqsfEgEGJNXQ4jEzsXAkwfQLFfgt47O3IpkUn0AxrQzutJDOcC28Uxp
raMVTVSlSkJIvaPuXJxdZ279tDMwZffILBfKCJGACT5V5/4WEqDkrF+uuF9/oxm2
5SVL8TvUmXB/3hX4UoaXtxAhuyOdhh1kyyZSpw9BPPR/8bc/wUYERh7+7JXLKHpd
ueeu3znfIX4dDeti8B3xYvvE8kGZjxFN1cC3zc3JsD0IVu1LkyiAa93P4LPEvAwG
Fw1LqmGiiqw9JM/tzc6kYkZXylFzCrSVf2exP+/tEvM=
-----END RSA PRIVATE KEY-----
```

11.9 show crypto certificate mycertificate

The **show crypto certificate mycertificate** Privileged EXEC mode command displays the device SSL certificates.

Syntax

show crypto certificate mycertificate [*number*]

Parameters

number—Specifies the certificate number. (Range: 1–3)

Default Configuration

Certificate number 1.

Command Mode

Privileged EXEC mode

Example

The following example displays SSL certificate # 1 present on the device.

```
switchxxxxxx# show crypto certificate mycertificate
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

12 Web Server Commands

12.1 ip http server

Use the **ip http server** Global Configuration mode command to enable configuring and monitoring the device from a web browser. Use the **no** form of this command to disable this function.

Syntax

ip http server

no ip http server

Parameters

N/A

Default Configuration

HTTP server is enabled.

Command Mode

Global Configuration mode

Example

The following example enables configuring the device from a web browser.

```
switchxxxxxx(config)# ip http server
```

12.2 ip http port

The **ip http port** Global Configuration mode command specifies the TCP port used by the web browser interface. Use the **no** form of this command to restore the default configuration.

Syntax

ip http port *port-number*

no ip http port

Parameters

port *port-number*—For use by the HTTP server. (Range: 0–65534)

Default Configuration

The default port number is 80.

Command Mode

Global Configuration mode

Example
The following example configures the http port number as 100.

```
switchxxxxxx(config)# ip http port 100
```

12.3 ip http timeout-policy
Use the **ip http timeout-policy** Global Configuration mode command to set the interval for the system to wait for user input in http/https sessions before automatic logoff. Use the **no** form of this command to return to the default value.

Syntax
ip http timeout-policy *idle-seconds*

no ip http timeout-policy

Parameters
idle-seconds—Specifies the maximum number of seconds that a connection is kept open if no data is received or response data cannot be sent out. (Range: 0–86400)

Default Configuration
600 seconds

Command Mode
Global Configuration mode

User Guidelines
To specify no timeout, enter the **ip http timeout-policy 0** command.

Example
The following example configures the http timeout to be 1000 seconds.

```
switchxxxxxx(config)# ip http timeout-policy 1000
```

12.4 ip http secure-server
Use the **ip http secure-server** Global Configuration mode command to enable the device to be configured or monitored securely from a browser. Use the **no** form of this command to disable this function.

Syntax
ip http secure-server

no ip http secure-server

Parameters
N/A

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
After this command is used, you must generate a certificate using crypto certificate generate. If no certificate is generated, this command has no effect.

Example

```
switchxxxxxx(config)# ip http secure-server
```

12.5 ip http secure-port
Use the **ip http secure-port** Global Configuration mode command to specify the TCP port to be used by the secure web browser. To use the default port, use the **no** form of this command.

Syntax
ip http secure-port *port-number*

no ip http secure-port

Parameters
port-number—Port number for use by the HTTPS server (Range: 0–65534)

Default Configuration
The default port number is 443.

Command Mode
Global Configuration mode

Example

```
switchxxxxxx(config)# ip http secure-port 1234
```

12.6 ip https certificate
Use the **ip https certificate** Global Configuration mode command to configure the active certificate for HTTPS. Use the **no** form of this command to restore the default configuration.

Syntax
ip https certificate *number*

no ip https certificate

Parameters
number—Specifies the certificate number. (Range: 1–2)

Default Configuration
The default certificate number is 1.

Command Mode
Global Configuration mode

User Guidelines
First, use crypto certificate generate to generate one or two HTTPS certificates. Then use this command to specify which is the active certificate.

Example
The following example configures the active certificate for HTTPS.

```
switchxxxxxx(config)# ip https certificate 2
```

12.7 show ip http
The **show ip http** EXEC mode command displays the HTTP server configuration.

Syntax
show ip http

Command Mode
EXEC mode

Example
The following example displays the HTTP server configuration.

```
switchxxxxxx# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes
```

12.8 show ip https
The **show ip https** Privileged EXEC mode command displays the HTTPS server configuration.

Syntax
show ip https

Command Mode
Privileged EXEC mode

Example

The following example displays the HTTPS server configuration.

```
switchxxxxxx# show ip https
HTTPS server enabled
Port: 443
Interactive timeout: Follows the HTTP interactive timeout (10 minutes)
Certificate 1 is active
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
Certificate 2 is inactive
Issued by: self-signed
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: 1873B936 88DC3411 BC8932EF 782134BA
```

13 Teletype Network (Telnet), Secure Shell (SSH) and Secure Login (Slogin) Commands

13.1 ip telnet server

Use the **ip telnet server** Global Configuration mode command to enable the device to be configured from a Telnet server. Use the **no** form of this command to disable the device configuration from a Telnet server.

Syntax

ip telnet server

no ip telnet server

Default Configuration

Configuration from a Telnet server is Disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The device can be configured from an SSH server or Telnet (or both). To control the device configuration by SSH, use the ip ssh pubkey-auth Global Configuration mode command.

Example

The following example enables the device to be configured from a Telnet server.

```
switchxxxxxx(config)# ip telnet server
```

13.2 ip ssh server

The **ip ssh server** Global Configuration mode command enables the device to be configured from an SSH server. Use the **no** form of this command to disable the device configuration from an SSH server.

Syntax

ip ssh server

no ip ssh server

Default Configuration

Device configuration from an SSH server is disabled.

Command Mode
Global Configuration mode

User Guidelines
The device can be configured from an SSH server or Telnet (or both). To control the device configuration by SSH, use the ip telnet server Global Configuration mode command

If encryption keys are not generated, the SSH server is in standby until the keys are generated. To generate SSH server keys, use the crypto key generate dsa and crypto key generate rsa Global Configuration mode commands.

Example
The following example enables configuring the device from an SSH server.

```
switchxxxxxx(config)# ip ssh server
```

13.3 ip ssh port
The **ip ssh port** Global Configuration mode command specifies the port used by the SSH server. Use the **no** form of this command to restore the default configuration.

Syntax
ip ssh port *port-number*

no ip ssh port

Parameters
port-number—Specifies the port number to be used by the SSH server. (Range: 1–65535)

Default Configuration
The default port number is 22.

Command Mode
Global Configuration mode

Example
The following example specifies that port number 8080 is used by the SSH server.

```
switchxxxxxx(config)# ip ssh port 8080
```

13.4 ip ssh pubkey-auth
Use the **ip ssh pubkey-auth** Global Configuration mode command to enable public key authentication of incoming SSH sessions. Use the **no** form of this command to disable this function.

Syntax
ip ssh pubkey-auth

no ip ssh pubkey-auth

Default Configuration
Public Key authentication of incoming SSH sessions is disabled.

Command Mode
Global Configuration mode

User Guidelines
This command enables encrypting information using the public key. AAA authentication is must be configured as usual.

Example
The following example configures authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh pubkey-auth
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob
switchxxxxxx(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
```

13.5 crypto key pubkey-chain ssh
The **crypto key pubkey-chain ssh** Global Configuration mode command enters the SSH Public Key-chain Configuration mode. This mode is used to manually specify device public keys, such as SSH client public keys.

Syntax
crypto key pubkey-chain ssh

Default Configuration
Keys do not exist.

Command Mode
Global Configuration mode

User Guidelines
Use this command when you want to manually specify SSH client's public keys.

Example

The following example enters the SSH Public Key-chain Configuration mode and manually configures the RSA key pair for SSH public key-chain to the user ‘bob’.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob
switchxxxxxx(config-pubkey-key)# key-string rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

13.6 user-key

The **user-key** SSH Public Key-string Configuration mode command associates a username with an SSH public key that was manually configured. Use the **no** form of this command to remove an SSH public key.

Syntax

user-key *username {**rsa** | **dsa**}*

no user-key *username*

Parameters

- **username**—Specifies the remote SSH client username. (Length: 1–48 characters)
- **rsa**—Specifies that the RSA key pair is manually configured.
- **dsa**—Specifies that the DSA key pair is manually configured.

Default Configuration

No SSH public keys exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Follow this command with key-string to specify the key.

Note that after entering this command, the existing key is deleted even if no new key is defined by key-string.

Example

The following example enables manually configuring an SSH public key for SSH public key-chain **bob**.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

13.7 key-string

The **key-string** SSH Public Key-string Configuration mode command manually specifies an SSH public key.

Syntax

key-string *[**row** key-string*]

Parameters

- **row**—Specifies the SSH public key row by row.
- **key-string**—Specifies the key in UU-encoded DER format. UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH. (Length:0–160)

Default Configuration

Keys do not exist.

Command Mode

SSH Public Key-string Configuration mode

User Guidelines

Use the **key-string** SSH Public Key-string Configuration mode command without the **row** parameter to specify which SSH public key is to be interactively configured next. Enter a row with no characters to complete the command.

Use the **key-string row** SSH Public Key-string Configuration mode command to specify the SSH public key, row by row. Each row must begin with a **key-string row** command.

The UU-encoded DER format is the same format as in the authorized_keys file used by OpenSSH.

Example

The following example enters public key strings for SSH public key client ‘bob’.

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
```

```
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-pubkey-chain)# user-key bob rsa
switchxxxxxx(config-pubkey-key)# key-string row AAAAB3Nza
switchxxxxxx(config-pubkey-key)# key-string row C1yc2
```

13.8 show ip ssh

The **show ip ssh** Privileged EXEC mode command displays the SSH server configuration.

Syntax

show ip ssh

Command Mode

Privileged EXEC mode

Example

The following example displays the SSH server configuration.

```
switchxxxxxx# show ip ssh
SSH server enabled. Port: 22
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled.
Active incoming sessions:
IP Address   SSH Username    Version        Cipher     Auth Code
---------    -----------     -------        ------     ----------
172.16.0.1   John Brown      1.5            3DES       HMAC-SHA1
```

The following table describes the significant fields shown in the display.

Field	Description
IP Address	The client address
SSH Username	The user name
Version	The SSH version number
Cipher	The encryption type (3DES, Blowfish, RC4)
Auth Code	The authentication Code (HMAC-MD5, HMAC-SHA1)

13.9 show crypto key pubkey-chain ssh

The **show crypto key pubkey-chain ssh** Privileged EXEC mode command displays SSH public keys stored on the device.

Syntax

show crypto key pubkey-chain ssh ***[username*** *username] [**fingerprint** {**bubble-babble** | **hex**}*]

Parameters

- **username** *username*—Specifies the remote SSH client username. (Length: 1–48 characters)
- **fingerprint** {**bubble-babble** | **hex**}—Specifies the fingerprint display format. The possible values are:
  - **bubble-babble**—Specifies that the fingerprint is displayed in Bubble Babble format.
  - **hex**—Specifies that the fingerprint is displayed in hexadecimal format.

Default Configuration

The default fingerprint format is hexadecimal.

Command Mode

Privileged EXEC mode

Example

The following examples display SSH public keys stored on the device.

```
switchxxxxxx# show crypto key pubkey-chain ssh
Username
--------
bob
john
Fingerprint
-----------------------------------------------
9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
switchxxxxxx# show crypto key pubkey-chain ssh username bob
Username: bob
Key: 005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B
55D6AB22 04AEF1BA A54028A6 9ACC01C5 129D99E4
Fingerprint: 9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

14 Line Commands

14.1 line

The **line** Global Configuration mode command identifies a specific line for configuration and enters the Line Configuration command mode.

Syntax

line *{* | ***telnet*** | ***ssh}***

Parameters

- —Enters the terminal line mode.
- **telnet**—Configures the device as a virtual terminal for remote access (Telnet).
- **ssh**—Configures the device as a virtual terminal for secured remote access (SSH).

Command Mode

Global Configuration mode

Example

The following example configures the device as a virtual terminal for remote (Telnet) access.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)#
```

14.2 speed

The **speed** Line Configuration mode command sets the line baud rate. Use the **no** form of this command to restore the default configuration.

Syntax

speed *bps*

no speed

Parameters

bps—Specifies the baud rate in bits per second (bps). Possible values are 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

Default Configuration

The default speed is 115200 bps.

Command Mode

Line Configuration mode

User Guidelines
The configured speed is applied when Autobaud is disabled. This configuration applies to the current session only.

Example
The following example configures the line baud rate as 9600 bits per second.

```
switchxxxxxx(config-line)# speed 9600
```

14.3 autobaud
The **autobaud** Line Configuration mode command sets the line for automatic baud rate detection (autobaud). Use the **no** form of this command to disable automatic baud rate detection.

Syntax
autobaud

no autobaud

Default Configuration
Automatic baud rate detection is enabled.

Command Mode
Line Configuration mode

User Guidelines
To start communication using Autobaud, press the **Enter** key twice.

Example
The following example enables autobaud.

```
switchxxxxxx(config)# line
switchxxxxxx(config-line)# autobaud
```

14.4 exec-timeout
The **exec-timeout** Line Configuration mode command sets the session idle time interval, during which the system waits for user input before automatic logoff. Use the **no** form of this command to restore the default configuration.

Syntax
exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameters
- **minutes**—Specifies the number of minutes. (Range: 0-65535)
- **seconds**—Specifies the number of seconds. (Range: 0-59)

Default Configuration
The default idle time interval is 10 minutes.

Command Mode
Line Configuration mode

Example
The following example sets the HTTP session idle time interval before automatic logoff to 20 minutes and 10 seconds.

```
switchxxxxxx(config)# line
switchxxxxxx(config-line)# exec-timeout 20 10
```

14.5 show line
The **show line** EXEC mode command displays line parameters.

Syntax
show line ***[*** | ***telnet*** | ***ssh]***

Parameters
- —Displays the configuration.
- **telnet**—Displays the Telnet configuration.
- **ssh**—Displays the SSH configuration.

Default Configuration
If the line is not specified, all line configuration parameters are displayed.

Command Mode
EXEC mode

Example
The following example displays the line configuration.

```
switchxxxxxx# show line
 configuration:
Interactive timeout: Disabled
History: 10
Baudrate: 9600
Databits: 8
Parity: none
Stopbits: 1
Telnet configuration:
Telnet is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
```

```
SSH configuration:
SSH is enabled.
Interactive timeout: 10 minutes 10 seconds
History: 10
```

15 Authentication, Authorization and Accounting (AAA) Commands

15.1 aaa authentication login

Use the **aaa authentication login** Global Configuration mode command to set one or more authentication methods to be applied during login. A list of authentication methods may be assigned a list name, and this list name can be used in login authentication . Use the **no** form of this command to restore the default authentication method.

Syntax

aaa authentication login *{**default** | list-name} method1* [*method2*...]

aaa authentication login *list-name method1 method2...*

no aaa authentication login *{**default** | list-name}*

Parameters

- **default**—Uses the authentication methods that follow this argument as the default method list when a user logs in (this list is unnamed).
- **list-name**—Specifies a name of a list of authentication methods activated when a user logs in. (Length: 1–12 characters)
- **method1 [method2...]**—Specifies a list of methods that the authentication algorithm tries (in the given sequence). Each additional authentication method is used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line. Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the locally-defined usernames for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

If no methods are specified, the default are the locally-defined users and passwords. This is the same as entering the command **aaa authentication login local**.

Note

If no authentication method is defined, console users can log in without any authentication verification.

Command Mode
Global Configuration mode

User Guidelines
Create a list of authentication methods by entering this command with the *list-name* parameter where *list-name* is any character string. The method arguments identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created with this command are used with login authentication .

no aaa authentication login *list-name* deletes a list-name only if it has not been referenced by another command.

Example
The following example sets the authentication login methods for the console.

```
switchxxxxxx (config)# aaa authentication login authen-list radius local
none
switchxxxxxx (config)#line console
switchxxxxxx (config-line)#login authentication authen-list
```

15.2 aaa authentication enable
The **aaa authentication enable** Global Configuration mode command sets one or more authentication methods for accessing higher privilege levels. A user, who logons with a lower privilege level, must pass these authentication methods to access a higher level.

To restore the default authentication method, use the **no** form of this command.

Syntax
aaa authentication enable {***default*** | *list-name*} *method* [*method2*...]

no aaa authentication enable {***default*** | *list-name*}

Parameters
- **default**—Uses the listed authentication methods that follow this argument as the default method list, when accessing higher privilege levels.
- **list-name** —Specifies a name for the list of authentication methods activated when a user accesses higher privilege levels. (Length: 1–12 characters)
- **method [method2...]**—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

Keyword	Description
radius	Uses the list of all RADIUS servers for authentication. Uses username "$enabx$." where x is the privilege level.
tacacs	Uses the list of all TACACS servers for authentication. Uses username "$enabx$." where x is the privilege level.

Default Configuration

The enable password command defines the default authentication login method. This is the same as entering the command **aaa authentication enable default enable**.

On a console, the enable password is used if a password exists. If no password is set, authentication still succeeds. This is the same as entering the command **aaa authentication enable default enable none**.

Command Mode

Global Configuration mode

User Guidelines

Create a list by entering the **aaa authentication enable** *list-name method1 [method2...]* command where *list-name* is any character string used to name this list. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence.

The default and list names created by this command are used with enable authentication.

All **aaa authentication enable default** requests sent by the device to a RADIUS or TACACS+ server include the username **$enabx$**., where **x** is the requested privilege level.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds even if all methods return an error.

no aaa authentication enable *list-name* deletes list-name if it has not been referenced.

Example

The following example sets the enable password for authentication for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

15.3 login authentication

The **login authentication** Line Configuration mode command specifies the login authentication method list for a remote Telnet or console session. Use the **no** form of this command to restore the default authentication method.

Syntax

login authentication *{**default** | list-name}*

no login authentication

Parameters

- **default**—Uses the default list created with the **aaa authentication login** command.
- **list-name**—Uses the specified list created with aaa authentication login.

Default Configuration

The default is the aaa authentication login command default.

Command Mode

Line Configuration mode

Examples

Example 1 - The following example specifies the login authentication method as the default method for a console session.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication default
```

Example

Example 2 - The following example sets the authentication login methods for the console as a list of methods.

```
switchxxxxxx (config)# aaa authentication login authen-list radius local
none
switchxxxxxx (config)#line console
switchxxxxxx (config-line)#login authentication authen-list
```

15.4 enable authentication

The **enable authentication** Line Configuration mode command specifies the authentication method for accessing a higher privilege level from a remote Telnet or console. Use the **no** form of this command to restore the default authentication method.

Syntax

enable authentication *{**default** | list-name}*

no enable authentication

Parameters

- **default**—Uses the default list created with the aaa authentication enable command.
- **list-name**—Uses the specified list created with the aaa authentication enable command.

Default Configuration

The default is the aaa authentication enable command default.

Command Mode

Line Configuration mode

Example

Example 1 - The following example specifies the authentication method as the default method when accessing a higher privilege level from a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication default
```

Example 2 - The following example sets a list of authentication methods for accessing higher privilege levels.

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

15.5 ip http authentication

The **ip http authentication** Global Configuration mode command specifies authentication methods for HTTP server access. Use the **no** form of this command to restore the default authentication method.

Syntax

ip http authentication aaa login-authentication *method1 [method2...]*

no ip http authentication aaa login-authentication

Parameters

method [method2...]—Specifies a list of methods that the authentication algorithm tries, in the given sequence. The additional authentication methods are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to ensure that the authentication succeeds, even if all methods return an error. Select one or more methods from the following list:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS+ servers for authentication.

Default Configuration

The local user database is the default authentication login method. This is the same as entering the **ip http authentication local** command.

Command Mode

Global Configuration mode

User Guidelines
The command is relevant for HTTP and HTTPS server users.

Example
The following example specifies the HTTP access authentication methods.

```
switchxxxxxx(config)# ip http authentication aaa login-authentication
radius local none
```

15.6 show authentication methods
The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax
show authentication methods

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the authentication configuration.

```
switchxxxxxx# show authentication methods
Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Console_Login: Line, None
Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Console_Enable: Enable, None
Line                  Login Method List    Enable Method List
--------------        -----------------    ------------------
Console               Console_Login        Console_Enable
Telnet                Default              Default
SSH                   Default              Default
HTTP: Radius, local
HTTPS: Radius, local
Dot1x: Radius
```

15.7 password

Use the **password** Line Configuration mode command to specify a password on a line (also known as an access method, such as a console or Telnet). Use the **no** form of this command to return to the default password.

Syntax

password *password* ***[encrypted]***

no password

Parameters

- **password**—Specifies the password for this line. (Length: 0–159 characters)
- **encrypted**—Specifies that the password is encrypted and copied from another device configuration.

Default Configuration

No password is defined.

Command Mode

Line Configuration mode

Example

The following example specifies the password ‘secret’ on a console.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secret
```

15.8 enable password

Use the **enable password** Global Configuration mode command to set a local password to control access to normal and privilege levels. Use the **no** form of this command to return to the default password.

When the administrator configures a new **enable** password, this password is encrypted automatically and saved to the configuration file. No matter how the password was entered, it appears in the configuration file with the keyword **encrypted** and the encrypted value.

If the administrator wants to manually copy a password that was configured on one switch (for instance, switch B) to another switch (for instance, switch A), the administrator must add **encrypted** in front of this encrypted password when entering the **enable** command in switch A. In this way, the two switches will have the same password.

Syntax

enable password ***[level*** *privilege-level] {unencrypted-password* | ***encrypted*** *encrypted-password}*

no enable password ***[level*** *level]*

Parameters

- **level** *privilege-level*—Level for which the password applies. If not specified the level is 15. (Range: 1–15)

- **password** *unencrypted-password*—Password for this level. (Range: 0–159 chars)
- **password encrypted** *encrypted-password*—Specifies that the password is encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)

Default Configuration

Default for **level** is 15.

Passwords are encrypted by default.

Command Mode

Global Configuration mode

User Guidelines

Passwords are encrypted by default. You only are required to use the **encrypted** keyword when you are actually entering an encrypted keyword.

Example

The first command sets an unencrypted password for level 7 (it will be encrypted in the configuration file).

The second command sets a password that has already been encrypted. It will copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# enable password level 7 let-me-in
switchxxxxxx(config)# enable password level 15 encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

15.9 username

Use the **username** Global Configuration mode command to establish a username-based authentication system. Use the **no** form to remove a user name.

Syntax

username *name {**nopassword** | **password** password | **privilege** privilege-level | unencrypted-password | **encrypted** encrypted-password}*

username *name*

no username *name*

Parameters

- **name**—The name of the user. (Range: 1–20 characters)
- **nopassword**—No password is required for this user to log in.
- **unencrypted-password**—The authentication password for the user. (Range: 1–159)
- **encrypted** *encrypted-password*—Specifies that the password is encrypted. Use this keyword to enter a password that is already encrypted (for instance that you copied from another the configuration file of another device). (Range: 1–40)
- **privilege** *privilege-level* —Privilege level for which the password applies. If not specified the level is 15. (Range: 1–15).

Default Configuration
No user is defined.

Command Mode
Global Configuration mode

Examples
Example 1 - Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
switchxxxxxx(config)# username tom privilege 15 password 1234
```

Example 2 - Sets a password for user jerry (level 15) that has already been encrypted. It will be copied to the configuration file just as it is entered. To use it, the user must know its unencrypted form.

```
switchxxxxxx(config)# username jerry privilege 15 encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

15.10 show user accounts
The **show user accounts** Privileged EXEC mode command displays information about the users local database.

Syntax
show user accounts

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays information about the users local database.

```
switchxxxxxx# show user accounts

Username         Privilege
--------         ---------
Bob              15
Robert           15
Smith            15
```

The following table describes the significant fields shown in the display:

Field	Description
Username	The user name.
Privilege	The user's privilege level.

15.11 aaa accounting login

Use the **aaa accounting login** command in Global Configuration mode to enable accounting of device management sessions. Use the **no** form of this command to disable accounting.

Syntax

aaa accounting login *start-stop group radius*

no aaa accounting login *start-stop group radius*

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of device management sessions (Telnet, serial and WEB but not SNMP).

It records only users that were identified with a username (e.g. a user that was logged in with a line password is not recorded).

If accounting is activated, the device sends a "start"/"stop" messages to a Radius server when a user logs in / logs out respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

The following table describes the supported Radius accounting attributes values, and when they are sent by the switch.

Name	Start	Stop	Description
User-Name (1)	Yes	Yes	User's identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the Radius server.
Class (25)	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.

Called-Station-ID (30)	Yes	Yes	The switch IP address that is used for the management session.
Calling-Station-ID (31)	Yes	Yes	The user IP address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicates how long the user was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.

Example

```
switchxxxxxx(config)# aaa accounting login start-stop group radius
```

15.12 aaa accounting dot1x

To enable accounting of 802.1x sessions, use the **aaa accounting dot1x** Global Configuration mode command. Use the **no** form of this command to disable accounting.

Syntax

aaa accounting dot1x *start-stop group radius*

no aaa accounting dot1x *start-stop group radius*

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

This command enables the recording of 802.1x sessions.

If accounting is activated, the device sends a “start”/“stop” messages to a Radius server when a user logs in / logs out to the network, respectively.

The device uses the configured priorities of the available Radius servers in order to select the Radius server.

If a new supplicant replaces an old supplicant (even if the port state remains authorized), the software sends a “stop” message for the old supplicant and a “start” message for the new supplicant.

In multiple sessions mode (dot1x multiple-hosts authentication), the software sends “start”/“stop” messages for each authenticated supplicant.

In multiple hosts mode (dot1x multiple-hosts), the software sends “start”/“stop” messages only for the supplicant that has been authenticated.

The software does not send “start”/“stop” messages if the port is force-authorized.

The software does not send “start”/“stop” messages for hosts that are sending traffic on the guest VLAN or on the unauthenticated VLANs.

The following table describes the supported Radius accounting Attributes Values and when they are sent by the switch.

Name	Start	Stop	Description
User-Name (1)	Yes	Yes	Supplicant’s identity.
NAS-IP-Address (4)	Yes	Yes	The switch IP address that is used for the session with the Radius server.
NAS-Port (5)	Yes	Yes	The switch port from where the supplicant has logged in.
Class (25)	Yes	Yes	Arbitrary value is included in all accounting packets for a specific session.
Called-Station-ID (30)	Yes	Yes	The switch MAC address.
Calling-Station-ID (31)	Yes	Yes	The supplicant MAC address.
Acct-Session-ID (44)	Yes	Yes	A unique accounting identifier.
Acct-Authentic (45)	Yes	Yes	Indicates how the supplicant was authenticated.
Acct-Session-Time (46)	No	Yes	Indicated how long the supplicant was logged in.
Acct-Terminate-Cause (49)	No	Yes	Reports why the session was terminated.
Nas-Port-Type (61)	Yes	Yes	Indicates the supplicant physical port type.

Example

```
switchxxxxxx(config)# aaa accounting dot1x start-stop group radius
```

15.13 show accounting

The **show accounting** EXEC mode command displays information about the accounting status.

Syntax

show accounting

Parameters

N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example displays information about the accounting status.

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

15.14 passwords complexity enable
Use the **passwords complexity enable** Global Configuration mode command to enforce minimum password complexity. The **no** form of this command disables enforcing password complexity.

Syntax
passwords complexity enable

no passwords complexity enable

Parameters

Parameters
N/A

Default Configuration

Disabled

Command Mode
Global Configuration mode

User Guidelines
If password complexity is enabled **by default**, the user is forced to enter a password that:

- Has a minimum length of 8 characters.
- Contains characters from at least 3 character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Are different from the current password.
- Contains no character that is repeated more than 3 times consecutively.
- Does not repeat or reverse the user name or any variant reached by changing the case of the characters.
- Does not repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

You can control the above attributes of password complexity with specific commands described in this section.

If you have previously configured other complexity settings, then those settings are used. This command does not wipe out the other settings. It works only as a toggle.

Example

The following example configures requiring complex passwords that fulfill the minimum requirements specified in the User Guidelines above.

```
switchxxxxxx(config)# passwords complexity enable
switchxxxxxx#show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
Minimal classes: 3
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
New password must be different than the manufacturer name: Enabled
switchcc293e#
```

15.15 passwords complexity <attributes>

Use the **passwords complexity <attributes>** Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the **no** form of these commands to return to default.

Syntax

passwords complexity *min-length* *number*

no passwords complexity *min-length*

passwords complexity *min-classes* *number*

no passwords complexity *min-classes*

passwords complexity *not-current*

no passwords complexity *not-current*

passwords complexity *no-repeat* *number*

no password complexity *no-repeat*

passwords complexity *not-username*

no passwords complexity *not-username*

Parameters

- **min-length** *number*—Sets the minimal length of the password. (Range: 0–64)
- **min-classes** *number*—Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 0–4)
- **not-current**—Specifies that the new password cannot be the same as the current password.

- **no-repeat** *number*—Specifies the maximum number of characters in the new password that can be repeated consecutively. Zero specifies that there is no limit on repeated characters. (Range: 0–16)
- **not-username**—Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.
- **not-manufacturer-name**—Specifies that the password cannot repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

Default Configuration
The minimal length is 8.

The number of classes is 3.

The default for no-repeat is 3.

All the other controls are enabled by default.

Command Mode
Global Configuration mode

Example
The following example configures the minimal required password length to 8 characters.

```
switchxxxxxx (config)# passwords complexity min-length 8
```

15.16 passwords min-length
The **passwords min-length** Global Configuration mode command configures the minimal password length in the local database. Use the **no** form of this command to remove the restriction.

Syntax
passwords min-length *length*

no passwords min-length

Parameters
length—Specifies the minimal length required for passwords. (Range: 8-64)

Default Configuration
There is no minimal length requirement until this command is executed.

Command Mode
Global Configuration mode

User Guidelines
The setting is relevant to local user passwords, line passwords, and enable passwords.

The software checks the minimum length requirement when defining a password in an unencrypted format, or when a user tries to log in.

Note that if a password is inserted in encrypted format, the minimum length requirement is checked during user login only.

Passwords that were defined before defining the minimum length requirement are only checked during user login.

Example
The following example configures the minimal required password length to 8 characters.

```
switchxxxxxx (config)# passwords min-length 8
```

15.17 passwords aging
Use the **passwords aging** Global Configuration mode command to enforce password aging. Use the **no** form of this command to return to default.

Syntax
passwords aging *days*

no passwords aging

Parameters
days—Specifies the number of days before a password change is forced. You can use 0 to disable aging. (Range: 0–365)

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
Aging is relevant only to users of the local database with privilege level 15 and to “enable” a password of privilege level 15.

Example
The following example configures the aging time to be 24 days.

```
switchxxxxxx (config)# passwords aging 24
```

15.18 passwords history
The **passwords history** Global Configuration mode command configures the number of password changes required before a password can be reused. Use the **no** form of this command to remove the requirement.

Syntax
passwords history *number*

no passwords history

Parameters
number—Specifies the number of password changes required before a password can be reused. (Range: 1–8)

Default Configuration
Password history is disabled.

Command Mode
Global Configuration mode

User Guidelines
The setting is relevant to local users' passwords, line passwords and enable passwords.

Password history is not checked during a configuration download.

The password history is kept even if the password history check is disabled.

The password history for a user is kept as long as the user is defined.

Example
The following example sets the number of password changes required before a password can be reused to 10.

```
switchxxxxxx(config)# passwords history 10
```

15.19 show passwords configuration
The **show passwords configuration** Privileged EXEC mode command displays information about the password management configuration.

Syntax
show passwords configuration

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example

```
switchxxxxxx#show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
Minimal length: 3 characters
Minimal classes: 3
```

```
New password must be different than the current: Enabled
Maximum consecutive same characters: 3
New password must be different than the user name: Enabled
New password must be different than the manufacturer name: Enabled
switchcc293e#
```

The following table describes the significant fields shown in the display:

Field	Description
Minimal length	The minimal length required for passwords in the local database.
Minimal character classes	The minimal number of different types of characters (special characters, integers and so on) required to be part of the password.
Maximum number of repeated characters	The maximum number of times a singe character can be repeated in the password.
Level	The applied password privilege level.
Aging	The password aging time in days.

15.20 show users login-history

The **show users login-history** Privileged EXEC mode command displays information about the user's login history.

Syntax

show users login-history ***[username*** *name]*

Parameters

name—Name of the user. (Range: 1–20 characters)

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays information about the users' login history.

```
switchxxxxxx# show users login-history
File save: Enabled.

Login Time              Username     Protocol      Location
--------------------    ----------   ----------    ------------
Jan 18 2004 23:58:17    Robert       HTTP          172.16.1.8
Jan 19 2004 07:59:23    Robert       HTTP          172.16.0.8
Jan 19 2004 08:23:48    Bob          Serial
Jan 19 2004 08:29:29    Robert       HTTP          172.16.0.8
Jan 19 2004 08:42:31    John         SSH           172.16.0.1
Jan 19 2004 08:49:52    Betty        Telnet        172.16.1.7
```

16 Remote Authentication Dial-In User Service (RADIUS) Commands

16.1 radius-server host

Use the **radius-server host** Global Configuration mode command to configure a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.

Syntax

radius-server host *{ip-address | hostname}* ***[auth-port*** *auth-port-number] [acct-port acct-port-number]* ***[timeout*** *timeout]* ***[retransmit*** *retries]* ***[deadtime*** *deadtime]* ***[key*** *key-string]* ***[source*** *{source-ip}]* ***[priority*** *priority]* ***[usage*** *{login | 802.1x | all}*]

no radius-server host {*ip-address* | *hostname*}

Parameters

- **ip-address**—Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions
- **hostname**—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)
- **auth-port** *auth-port-number*—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- **acct-port-number**—Port number for accounting requests. The host is not used for accountings if set to 0. If unspecified, the port number defaults to 1813.
- **timeout** *timeout*—Specifies the timeout value in seconds. (Range: 1–30)
- **retransmit** *retries*—Specifies the retransmit value. (Range: 1–10)
- **deadtime** *deadtime*—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
- **key** *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters)
- **source** *source-ip*—Specifies the source IPv4 or IPv6 address to use for communication. 0.0.0.0 is interpreted as a request to use the IP address of the outgoing IP interface.
- **priority** *priority*—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- **usage** {**login** | **802.1x** | **all**}—Specifies the RADIUS server usage type. The possible values are:
  - **login**—Specifies that the RADIUS server is used for user login parameters authentication.
  - **802.1x**—Specifies that the RADIUS server is used for 802.1x port authentication.
  - **all**—Specifies that the RADIUS server is used for user login authentication and 802.1x port authentication.

Default Configuration

The default authentication port number is 1812.

If **timeout** is not specified, the global value (set in radius-server timeout) is used.

If **retransmit** is not specified, the global value (set in radius-server retransmit) is used.

If **key-string** is not specified, the global value (set in radius-server key) is used.

If the **source** value is not specified, the global value (set in radius-server source-ip or radius-server source-ipv6) is used.

If a parameter was not set in one of the above commands, the default for that command is used. For example, if a timeout value was not set in the current command or in radius-server timeout, the default timeout for radius-server timeout is used.

The default usage type is **all**.

Command Mode
Global Configuration mode

User Guidelines
To specify multiple hosts, this command is used for each host.

The **source** parameter address type (IPv4 or IPv6) must be the same as that of the **host** IP address type.

Example
The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
switchxxxxxx(config)# radius-server host 192.168.10.1 auth-port 20
timeout 20
```

16.2 radius-server key
Use the **radius-server key** Global Configuration mode command to set the authentication and encryption key for RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to restore the default configuration.

Syntax
radius-server key [*key-string*]

no radius-server key

Parameters
key-string—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)

Default Configuration
The key-string is an empty string.

Command Mode
Global Configuration mode

Example
The following example defines the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.

```
switchxxxxxx(config)# radius-server key enterprise-server
```

16.3 radius-server retransmit
Use the **radius-server retransmit** Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

Syntax
radius-server retransmit *retries*

no radius-server retransmit

Parameters
retransmit *retries*—Specifies the retransmit value. (Range: 1–10)

Default Configuration
The software searches the list of RADIUS server hosts 3 times.

Command Mode
Global Configuration mode

Example
The following example configures the number of times the software searches all RADIUS server hosts as 5.

```
switchxxxxxx(config)# radius-server retransmit 5
```

16.4 radius-server source-ip
Use the **radius-server source-ip** Global Configuration mode command to specify the source IP address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax
radius-server source-ip {*source-ip-address*}

no radius-server source-ip {*source-ip-address*}

Parameters
source-ip-address—Specifies the source IP address.

Default Configuration
The source IP address is the IP address of the outgoing IP interface.

Command Mode
Global Configuration mode

User Guidelines
If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

Example
The following example configures the source IP address used for communication with all RADIUS servers to 10.1.1.1.

```
switchxxxxxx(config)# radius-server source-ip 10.1.1.1
```

16.5 radius-server source-ipv6
Use the **radius-server source-ipv6** Global Configuration mode command to specify the source IPv6 address used for communication with RADIUS servers. Use the no form of this command to restore the default configuration.

Syntax
radius-server source-ipv6 {*source*}

no radius-server source-ipv6 {*source*}

Parameters
source—Specifies the source IPv6 address.

Default Configuration
The source IP address is the IP address of the outgoing IP interface.

Command Mode
Global Configuration mode

User Guidelines
If there is no available IP interface of the configured IP source address, an error message is issued when attempting to communicate with the IP address.

Example
The following example configures the source IP address used for communication with all RADIUS servers to 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

```
switchxxxxxx(config)# radius-server source-ipv6
3ffe:1900:4545:3:200:f8ff:fe21:67cf
```

16.6 radius-server timeout
Use the **radius-server timeout** Global Configuration mode command to set how long the device waits for a server host to reply. Use the **no** form of this command to restore the default configuration.

Syntax
radius-server timeout *timeout-seconds*

no radius-server timeout

Parameters
timeout *timeout-seconds*—Specifies the timeout value in seconds. (Range: 1–30)

Default Configuration
The default timeout value is 3 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
switchxxxxxx(config)# radius-server timeout 5
```

16.7 radius-server deadtime
Use the **radius-server deadtime** Global Configuration mode command to configure how long unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the **no** form of this command to restore the default configuration.

Syntax
radius-server deadtime *deadtime*

no radius-server deadtime

Parameters
deadtime—Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)

Default Configuration
The default deadtime interval is 0.

Command Mode
Global Configuration mode

Example
The following example sets all RADIUS server deadtimes to 10 minutes.

```
switchxxxxxx(config)# radius-server deadtime 10
```

16.8 show radius-servers

Use the **show radius-servers** Privileged EXEC mode command to display the RADIUS server settings.

Syntax

show radius-servers

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server settings.

```
switchxxxxxx# show radius-servers

            Port   Port   Time                    Dead     Source
IP address  Auth   Acct   Out      Retransmision  time     IP       Priority  Usage
----------  ----   ----   -----    -------------  ------   ------   --------  -----
172.16.1.1  1812   1813   Global   Global         Global   Global   1         All
172.16.1.2  1812   1813   11       8              Global   Global   2         All


Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IP: 172.16.8.1
```

17 Terminal Access Controller Access-Control System Plus (TACACS+) Commands

17.1 tacacs-server host

Use the **tacacs-server host** Global Configuration mode command to specify a TACACS+ host. Use the **no** form of this command to delete the specified TACACS+ host.

Syntax

tacacs-server host {*ip-address* | *hostname*} *[single-connection] [**port** port-number] [**timeout** timeout] [**key** key-string] [**source** {source-ip}] [**priority** priority]*

no tacacs-server host {*ip-address* | *hostname*}

Parameters

- **host** *ip-address*—Specifies the TACACS+ server host IP address.
- **host** *hostname*—Specifies the TACACS+ server host name. (Length: 1?158 characters. Maximum label length of each part of the host name: 63 characters)
- **single-connection**—Specifies that a single open connection is maintained between the device and the daemon, instead of the device opening and closing a TCP connection to the daemon each time it communicates.
- **port** *port-number*—Specifies the TACACS server TCP port number. If the port number is 0, the host is not used for authentication. (Range: 0-65535)
- **timeout** *timeout*—Specifies the timeout value in seconds. (Range: 1-30)
- **key** *key-string*—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. To specify an empty string, enter "". (Length: 0-128 characters). This key is set in tacacs-server key.
- **source** *source-ip*—Specifies the source IP address to use for the communication. 0.0.0.0 indicates a request to use the outgoing IP interface IP address.
- **priority** *priority*—Specifies the order in which the TACACS+ servers are used, where 0 is the highest priority. (Range: 0-65535)

Default Configuration

No TACACS+ host is specified.

The default **port-number** is 49.

The default authentication port number is 1812.

If **timeout** is not specified, the global value (set in tacacs-server timeout) is used.

If **key-string** is not specified, the global value (set in tacacs-server key) is used.

If the **source** value is not specified, the global value (set in tacacs-server source-ip) is used.

If a parameter was not set in one of the above commands, the default for that command is used. For example, if a timeout value was not set in the current command or in tacacs-server timeout, the default timeout for tacacs-server timeout is used.

Command Mode
Global Configuration mode

User Guidelines
Multiple **tacacs-server host** commands can be used to specify multiple hosts.

Example
The following example specifies a TACACS+ host.

```
switchxxxxxx(config)# tacacs-server host 172.16.1.1
```

17.2 tacacs-server key
Use the **tacacs-server key** Global Configuration mode command to set the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon. Use the **no** form of this command to disable the key.

Syntax
tacacs-server key *key-string*

no tacacs-server key

Parameters
key-string—Specifies the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ daemon. (Length: 0–128 characters)

Default Configuration
The default key is an empty string.

Command Mode
Global Configuration mode

Example
The following example sets Enterprise as the authentication encryption key for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server key enterprise
```

17.3 tacacs-server timeout
Use the **tacacs-server timeout** Global Configuration mode command to set the interval during which the device waits for a TACACS+ server to reply. Use the **no** form of this command to restore the default configuration.

Syntax
tacacs-server timeout *timeout*

no tacacs-server timeout

Parameters
timeout—Specifies the timeout value in seconds. (Range: 1-30)

Default Configuration
The default timeout value is 5 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the timeout value to 30 for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server timeout 30
```

17.4 tacacs-server source-ip
Use the **tacacs-server source-ip** Global Configuration mode command to configure the source IP address to be used for communication with TACACS+ servers. Use the no form of this command to restore the default configuration.

Syntax
tacacs-server source-ip {*source*}

no tacacs-server source-ip {*source*}

Parameters
source—Specifies the source IP address. (Range: Valid IP address)

Default Configuration
The default source IP address is the outgoing IP interface address.

Command Mode
Global Configuration mode

User Guidelines
If the configured IP source address has no available IP interface, an error message is issued when attempting to communicate with the IP address.

Example
The following example specifies the source IP address for all TACACS+ servers.

```
switchxxxxxx(config)# tacacs-server source-ip 172.16.8.1
```

17.5 show tacacs
Use the **show tacacs** Privileged EXEC mode command to display configuration and statistical information for a TACACS+ server.

Syntax
show tacacs [*ip-address*]

Parameters
ip-address—Specifies the TACACS+ server name or IP address.

Default Configuration
If **ip-address** is not specified, information for all TACACS+ servers is displayed.

Command Mode
Privileged EXEC mode

Example
The following example displays configuration and statistical information for all TACACS+ servers.

```
switchxxxxxx# show tacacs

IP address     Status      Port   Single       Time     Source   Priority
                                  Connection   Out      IP
----------     ------      ----   ----------   -----    -----    ------
172.16.1.1     Connected   49     No           Global   Global   1

Global values
-------------
Time Out: 3
Source IP: 172.16.8.1
```

18 Syslog Commands

18.1 logging on

Use the **logging on** Global Configuration mode command to control error message logging. This command sends debug or error messages asynchronously to designated locations. Use the **no** form of this command to disable the logging.

Syntax

logging on

no logging on

Parameters

N/A

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

User Guidelines

The logging process controls the logging messages distribution at various destinations, such as the logging buffer, logging file or SYSLOG server. Logging on and off at these destinations can be individually configured using the logging buffered, logging file, and logging on Global Configuration mode commands. However, if the logging on command is disabled, no messages are sent to these destinations. Only the console receives messages.

Example

The following example enables logging error messages.

```
switchxxxxxx(config)# logging on
```

18.2 logging host

Use the **logging host** Global Configuration command to log messages to the specified SYSLOG server. Use the **no** form of this command to delete the SYSLOG server with the specified address from the list of SYSLOG servers.

Syntax

logging host *{ip-address | ipv6-address | hostname}* ***[port*** *port]* ***[severity*** *level]* ***[facility*** *facility]* ***[description*** *text]*

no logging host *{ipv4-address | ipv6-address | hostname}*

Parameters

- **ip-address**—IP address of the host to be used as a SYSLOG server. The IP address can be an IPv4, IPv6 or Ipv6z address. See IPv6z Address Conventions.
- **hostname**—Hostname of the host to be used as a SYSLOG server. Only translation to IPv4 addresses is supported. (Range: 1–158 characters. Maximum label size for each part of the host name: 63)
- ***port*** *port*—Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- ***severity*** *level*—Limits the logging of messages to the SYSLOG servers to a specified level: emergencies, alerts, critical, errors, warnings, notifications, informational, debugging.
- ***facility*** *facility*—The facility that is indicated in the message. It can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7. If unspecified, the port number defaults to local7.
- ***description*** *text*—Description of the SYSLOG server. (Range: Up to 64 characters)

Default Configuration

No messages are logged to a SYSLOG server.

if unspecified, the **severity level** defaults to Informational.

Command Mode

Global Configuration mode

User Guidelines

You can use multiple SYSLOG servers.

Examples

```
switchxxxxxx(config)# logging host 1.1.1.121
```

```
switchxxxxxx(config)# logging host 3000::100/SYSLOG1
```

18.3 logging console

Use the **logging console** Global Configuration mode command to limit messages logged to the console to messages to a specific severity level. Use the **no** form of this command to restore the default.

Syntax

logging console *level*

no logging console

Parameters

level—Specifies the severity level of logged messages displayed on the console. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

Informational.

Command Mode
Global Configuration mode

Example
The following example limits logging messages displayed on the console to messages with severity level **errors**.

```
switchxxxxxx(config)# logging console errors
```

18.4 logging buffered
Use the **logging buffered** Global Configuration mode command to limit the SYSLOG message display to messages with a specific severity level, and to define the buffer size (number of messages that can be stored). Use the **no** form of this command to cancel displaying the SYSLOG messages, and to return the buffer size to default.

Syntax
logging buffered [*buffer-size*] [*severity-level* | *severity-level-name*]

no logging buffered

Parameters
- **buffer-size**—Specifies the maximum number of messages stored in the history table. (Range: 20–400)
- **severity-level**—Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- **severity-level-name**—Specifies the severity level of messages logged in the buffer. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration
The default severity level is informational.

The default buffer size is 200.

Command Mode
Global Configuration mode

User Guidelines
All the SYSLOG messages are logged to the internal buffer. This command limits the messages displayed to the user.

Example
The following example shows two ways of limiting the SYSLOG message display from an internal buffer to messages with severity level **debugging**. In the second example, the buffer size is set to 100.

```
switchxxxxxx(config)# logging buffered debugging
switchxxxxxx(config)# logging buffered 100 7
```

18.5 clear logging

Use the **clear logging** Privileged EXEC mode command to clear messages from the internal logging buffer.

Syntax

clear logging

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

```
switchxxxxxx# clear logging
Clear logging buffer [confirm]
```

18.6 logging file

Use the **logging file** Global Configuration mode command to limit SYSLOG messages sent to the logging file to messages with a specific severity level. Use the **no** form of this command to cancel sending messages to the file.

Syntax

logging file *level*

no logging file

Parameters

level—Specifies the severity level of SYSLOG messages sent to the logging file. The possible values are: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging.

Default Configuration

The default severity level is **errors**.

Command Mode

Global Configuration mode

Example
The following example limits SYSLOG messages sent to the logging file to messages with severity level **alerts**.

```
switchxxxxxx(config)# logging file alerts
```

18.7 clear logging file
Use the **clear logging file** Privileged EXEC mode command to clear messages from the logging file.

Syntax
clear logging file

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example clears messages from the logging file.

```
switchxxxxxx# clear logging file
Clear Logging File [y/n]
```

18.8 aaa logging
Use the **aaa logging** Global Configuration mode command to enable logging AAA logins. Use the **no** form of this command to disable logging AAA logins.

Syntax
aaa logging *{login}*

no aaa logging *{login}*

Parameters
login—Enables logging messages related to successful AAA login events, unsuccessful AAA login events and other AAA login-related events.

Default Configuration
Enabled.

Command Mode
Global Configuration mode

User Guidelines
This command enables logging messages related to successful login events, unsuccessful login events and other login-related events. Other types of AAA events are not subject to this command.

Example
The following example enables logging AAA login events.

```
switchxxxxxx(config)# aaa logging login
```

18.9 file-system logging
Use the **file-system logging** Global Configuration mode command to enable logging file system events. Use the **no** form of this command to disable logging file system events.

Syntax
file-system logging *{**copy** | **delete-rename**}*

no file-system logging *{**copy** | **delete-rename**}*

Parameters
- **copy**—Specifies logging messages related to file copy operations.
- **delete-rename**—Specifies logging messages related to file deletion and renaming operations.

Default Configuration
Enabled.

Command Mode
Global Configuration mode

Example
The following example enables logging messages related to file copy operations.

```
switchxxxxxx(config)# file-system logging copy
```

18.10 management logging
Use the **management logging** Global Configuration mode command to enable logging Management Access List (ACL) deny events (rejected logins). Use the **no** form of this command to disable logging management access list events.

Syntax
management logging {***deny***}

no management logging {***deny***}

Parameters
deny—Enables logging messages related to management ACL deny actions (rejected logins).

Default Configuration
Logging management ACL deny events is enabled.

Command Mode
Global Configuration mode

User Guidelines
Other management ACL events are not subject to this command.

Example
The following example enables logging messages related to management ACL deny actions.

```
switchxxxxxx(config)# management logging deny
```

18.11 logging aggregation on
Use the **logging aggregation on** Global Configuration mode command to control aggregation of SYSLOG messages. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by logging aggregation aging-time). Use the **no** form of this command to disable aggregation of SYSLOG messages.

Syntax
logging aggregation on

no logging aggregation on

Parameters
N/A

Default Configuration
Enabled.

Command Mode
Global Configuration mode

Example
To turn off aggregation of SYSLOG messages:

```
switchxxxxxx(config)# no logging aggregation on
```

18.12 logging aggregation aging-time
Use the **logging aggregation aging-time** Global Configuration mode command to configure the aging time of the aggregated SYSLOG messages. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. Use the **no** form of this command to return to the default.

Syntax
logging aggregation aging-time *sec*

no logging aggregation aging-time

Parameters
aging-time *sec*—Aging time in seconds (Range: 15–3600)

Default Configuration
300 seconds.

Command Mode
Global Configuration mode

Example

```
switchxxxxxx(config)# logging aggregation aging-time 300
```

18.13 show logging
Use the **show logging** Privileged EXEC mode command to display the logging status and SYSLOG messages stored in the internal buffer.

Syntax
show logging

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays the logging status and the SYSLOG messages stored in the internal buffer.

```
switchxxxxxx# show logging
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200
Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
```

```
Application            Event                Status
--------------------   ----------------     ---------
AAA                    Login                Enabled
File system            Copy                 Enabled
File system            Delete-Rename        Enabled
Management ACL         Deny                 Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
01-Jan-2010 05:29:46 :%INIT-I-Startup: Warm Startup
01-Jan-2010 05:29:02 :%LINK-I-Up:  Vlan 1
01-Jan-2010 05:29:02 :%LINK-I-Up:  SYSLOG6
01-Jan-2010 05:29:02 :%LINK-I-Up:  SYSLOG7
01-Jan-2010 05:29:00 :%LINK-W-Down:  SYSLOG8
```

18.14 show logging file

Use the **show logging file** Privileged EXEC mode command to display the logging status and the SYSLOG messages stored in the logging file.

Syntax

show logging file

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example displays the logging status and the SYSLOG messages stored in the logging file.

```
switchxxxxxx# show logging file
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 61 Logged, 61 Displayed, 200
Max.
File Logging: Level error. File Messages: 898 Logged, 64 Dropped.
4 messages were not logged
Application filtering control
Application              Event                 Status
-----------------        ----------------      ---------
AAA                      Login                 Enabled
```

```
File system              Copy                    Enabled
File system              Delete-Rename           Enabled
Management ACL           Deny                    Enabled
Aggregation: Disabled.
Aggregation aging time: 300 Sec
01-Jan-2010 05:57:00 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error
01-Jan-2010 05:56:36 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error
01-Jan-2010 05:55:37 :%SSHD-E-ERROR: SSH error: key_read: type mismatch:
encoding error
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_read: key_from_blob
bgEgGnt9
z6NHgZwKI5xKqF7cBtdl1xmFgSEWuDhho5UedydAjVkKS5XR2... failed
01-Jan-2010 05:55:03 :%SSHD-E-ERROR: SSH error: key_from_blob: invalid key
type.
01-Jan-2010 05:56:34 :%SSHD-E-ERROR: SSH error: bad sigbloblen 58 !=
SIGBLOB_LEN
console#
```

18.15 show syslog-servers

Use the **show syslog-servers** Privileged EXEC mode command to display the SYSLOG server settings.

Syntax

show syslog-servers

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example provides information about the SYSLOG servers.

```
switchxxxxxx# show syslog-servers
Device Configuration
IP address    Port   Facility Severity  Description
------------- ----   --------- -------- --------------
1.1.1.121     514    local7    info
3000::100     514    local7    info
```

19 Remote Network Monitoring (RMON) Commands

19.1 show rmon statistics

Use the **show rmon statistics** EXEC mode command to display RMON Ethernet statistics.

Syntax

show rmon statistics *{interface-id}*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays RMON Ethernet statistics for gigabitethernet port `fe1/0/1`1.

```
switchxxxxxx# show rmon statistics fe1/0/11
Port fe1/0/11
Dropped: 0
Octets: 0                          Packets: 0
Broadcast: 0                       Multicast: 0
CRC Align Errors: 0                Collisions: 0
Undersize Pkts: 0                  Oversize Pkts: 0
Fragments: 0                       Jabbers: 0
64 Octets: 0                       65 to 127 Octets: 1
128 to 255 Octets: 1               256 to 511 Octets: 1
512 to 1023 Octets: 0              1024 to max Octets: 0
```

The following table describes the significant fields displayed.

Field	Description
Dropped	Total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped. It is the number of times this condition was detected.
Octets	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Field	Description
Broadcast	Total number of good packets received and directed to the broadcast address. This does not include multicast packets.
Multicast	Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	Total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	Best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	Total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	Total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	Total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	Total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to max	Total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).

19.2 rmon collection stats

Use the **rmon collection stats** Interface Configuration mode command to enable RMON MIB collecting history statistics (in groups) on an interface. Use the **no** form of this command to remove a specified RMON history group of statistics.

Syntax

rmon collection stats index ***[owner*** *ownername]* ***[buckets*** *bucket-number]* ***[interval*** *seconds]*

no rmon collection stats *index*

Parameters

- **index**—The requested group of statistics index.(Range: 1–65535)
- **owner** *ownername*—Records the name of the owner of the RMON group of statistics. If unspecified, the name is an empty string. (Range: Valid string)
- **buckets** *bucket-number*—A value associated with the number of buckets specified for the RMON collection history group of statistics. If unspecified, defaults to 50.(Range: 1–50)
- **interval** *seconds*—The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

Command Mode

Interface Configuration (Ethernet, Port-channel) mode. Cannot be configured for a range of interfaces (range context).

19.3 show rmon collection stats

Use the **show rmon collection stats** EXEC mode command to display the requested RMON history group statistics.

Syntax

show rmon collection stats *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example displays all RMON history group statistics.

```
switchxxxxxx# show rmon collection stats
Index   Interface   Interval   Requested   Granted     Owner
                               Samples     Samples
-----   ---------   --------   ---------   -------     -------
1       fe1/0/11    30         50          50          CLI
2       fe1/0/11    1800       50          50          Manager
```

The following table describes the significant fields shown in the display.

Field	Description
Index	An index that uniquely identifies the entry.
Interface	The sampled Ethernet interface.
Interval	The interval in seconds between samples.
Requested Samples	The requested number of samples to be saved.
Granted Samples	The granted number of samples to be saved.
Owner	The entity that configured this entry.

19.4 show rmon history

Use the **show rmon history** EXEC mode command to display RMON Ethernet history statistics.

Syntax

show rmon history *index {**throughput** | **errors** | **other**} [**period** seconds*]

Parameters

- **index**—Specifies the set of samples to display. (Range: 1–65535)
- **throughput**—Displays throughput counters.
- **errors**—Displays error counters.
- **other**—Displays drop and collision counters.
- **period** *seconds*—Specifies the period of time in seconds to display. (Range: 1–2147483647)

Command Mode

EXEC mode

Example

The following examples display RMON Ethernet history statistics for index 1

```
switchxxxxxx# show rmon history 1 throughput

Sample Set: 1                    Owner: CLI
Interface: fe1/0/11              Interval: 1800
Requested samples: 50            Granted samples: 50

Maximum table size: 500

Time                  Octets     Packets    Broadcast   Multicast    Util
--------------------  --------   -------    --------    ---------    ----
Jan 18 2005 21:57:00  303595962  357568     3289        7287         19%
Jan 18 2005 21:57:30  287696304  275686     2789        5878         20%
```

```
switchxxxxxx# show rmon history 1 errors

Sample Set: 1                    Owner: Me
Interface:fe1/0/11               Interval: 1800
Requested samples: 50            Granted samples: 50
```

```
Maximum table size: 500 (800 after reset)

Time                CRC       Under
                    Align     size      Oversize   Fragments   Jabbers
------------        -------   -----     --------   ---------   ----
Jan 18 2005
21:57:00            1         1         0          49          0
Jan 18 2005         1         1         0          27          0
21:57:30
```

```
switchxxxxxx# show rmon history 1 other

Sample Set: 1                   Owner: Me
Interface: fe1/0/11             Interval: 1800
Requested samples: 50           Granted samples: 50

Maximum table size: 500

Time                            Dropped   Collisions
--------------------            ------    ----------
Jan 18 2005 21:57:00            3         0
Jan 18 2005 21:57:30            3         0
```

The following table describes significant fields shown in the display:

Field	Description
Time	Date and Time the entry is recorded.
Octets	Total number of octets of data (including those in bad packets and excluding framing bits but including FCS octets) received on the network.
Packets	Number of packets (including bad packets) received during this sampling interval.
Broadcast	Number of good packets received during this sampling interval that were directed to the broadcast address.
Multicast	Number of good packets received during this sampling interval that were directed to a multicast address. This number does not include packets addressed to the broadcast address.
Utilization	Best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.

Field	Description
Oversize	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Fragments	Total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for etherHistoryFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	Number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Dropped	Total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. This number is not necessarily the number of packets dropped, it is the number of times this condition has been detected.
Collisions	Best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

19.5 rmon alarm

Use the **rmon alarm** Global Configuration mode command to configure alarm conditions. Use the **no** form of this command to remove an alarm.

Syntax

rmon alarm *index mib-object-id interval rising-threshold falling-threshold rising-event falling-event [**type** {**absolute** | **delta**}] [**startup** {**rising** | **rising-falling** | **falling**}] [**owner** name]*

no rmon alarm *index*

Parameters

- **index**—Specifies the alarm index. (Range: 1–65535)
- **mib-object-id**—Specifies the object identifier of the variable to be sampled. (Valid OID)
- **interval**—Specifies the interval in seconds during which the data is sampled and compared with rising and falling thresholds. (Range: 1–4294967295)
- **rising-threshold**—Specifies the rising threshold value. (Range: 0–4294967295)
- **falling-threshold**—Specifies the falling threshold value. (Range: 0–4294967295)
- **rising-event**—Specifies the index of the event triggered when a rising threshold is crossed. (Range: 0–65535)
- **falling-event**—Specifies the index of the event triggered when a falling threshold is crossed. (Range: 0–65535)
- **type** {**absolute** | **delta**}—Specifies the method used for sampling the selected variable and calculating the value to be compared against the thresholds. The possible values are:
  - **absolute**—Specifies that the selected variable value is compared directly with the thresholds at the end of the sampling interval.

  - **delta**—Specifies that the selected variable value of the last sample is subtracted from the current value, and the difference is compared with the thresholds.
- **startup** {**rising** | **rising-falling** | **falling**}—Specifies the alarm that may be sent when this entry becomes valid. The possible values are:
  - **rising**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to **rising-threshold**, a single rising alarm is generated.
  - **rising-falling**—Specifies that if the first sample (after this entry becomes valid) is greater than or equal to ***rising-threshold***, a single rising alarm is generated. If the first sample (after this entry becomes valid) is less than or equal to **falling-threshold**, a single falling alarm is generated.
  - **falling** —Specifies that if the first sample (after this entry becomes valid) is less than or equal to **falling-threshold**, a single falling alarm is generated.
- **owner** *name*—Specifies the name of the person who configured this alarm. (Valid string)

Default Configuration

The default method type is **absolute**.

The default **startup** direction is **rising-falling**.

If the owner **name** is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an alarm with index 1000, MIB object ID D-Link, sampling interval 360000 seconds (100 hours), rising threshold value 1000000, falling threshold value 1000000, rising threshold event index 10, falling threshold event index 10, absolute method type and rising-falling alarm.

```
switchxxxxxx(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000
1000000 1000000 10 20
```

19.6 show rmon alarm-table

Use the **show rmon alarm-table** EXEC mode command to display a summary of the alarms table.

Syntax

show rmon alarm-table

Command Mode

EXEC mode

Example
The following example displays the alarms table.

```
switchxxxxxx# show rmon alarm-table
Index      OID                      Owner
-----      ----------------------   -------
1          1.3.6.1.2.1.2.2.1.10.1   CLI
2          1.3.6.1.2.1.2.2.1.10.1   Manager
3          1.3.6.1.2.1.2.2.1.10.9   CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Index	An index that uniquely identifies the entry.
OID	Monitored variable OID.
Owner	The entity that configured this entry.

19.7 show rmon alarm
Use the **show rmon alarm** EXEC mode command to display alarm configuration.

Syntax
show rmon alarm *number*

Parameters
alarm *number*—Specifies the alarm index. (Range: 1–65535)

Command Mode
EXEC mode

Example
The following example displays RMON 1 alarms.

```
switchxxxxxx# show rmon alarm 1
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
```

```
Owner: CLI
```

The following table describes the significant fields shown in the display:

Field	Description
Alarm	Alarm index.
OID	Monitored variable OID.
Last Sample Value	Value of the statistic during the last sampling period. For example, if the sample type is **delta**, this value is the difference between the samples at the beginning and end of the period. If the sample type is **absolute**, this value is the sampled value at the end of the period.
Interval	Interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
Sample Type	Method of sampling the variable and calculating the value compared against the thresholds. If the value is **absolute**, the variable value is compared directly with the thresholds at the end of the sampling interval. If the value is **delta**, the variable value at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Startup Alarm	Alarm that is sent when this entry is first set. If the first sample is greater than or equal to the rising threshold, and startup alarm is equal to rising or rising-falling, then a single rising alarm is generated. If the first sample is less than or equal to the falling threshold, and startup alarm is equal falling or rising-falling, then a single falling alarm is generated.
Rising Threshold	Sampled statistic rising threshold. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated.
Falling Threshold	Sampled statistic falling threshold. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated.
Rising Event	Event index used when a rising threshold is crossed.
Falling Event	Event index used when a falling threshold is crossed.
Owner	Entity that configured this entry.

19.8 rmon event

Use the **rmon event** Global Configuration mode command to configure an event. Use the **no** form of this command to remove an event.

Syntax

rmon event *index {**none** | **log** | **trap** | **log-trap**} [**community** text] [**description** text] [**owner** name]*

no rmon event *index*

Parameters

- **index**—Specifies the event index. (Range: 1–65535)
- **none**— Specifies that no notification is generated by the device for this event.
- **log**—Specifies that a notification entry is generated in the log table by the device for this event.
- **trap**—Specifies that an SNMP trap is sent to one or more management stations by the device for this event.
- **log-trap**—Specifies that an entry is generated in the log table and an SNMP trap is sent to one or more management stations by the device for this event.
- **community text**—Specifies the SNMP community (password) used when an SNMP trap is sent. (Octet string;
  length: 0–127 characters)
- **description text**—Specifies a comment describing this event. (Length: 0–127 characters)
- **owner name**—Specifies the name of the person who configured this event. (Valid string)

Default Configuration

If the owner name is not specified, it defaults to an empty string.

Command Mode

Global Configuration mode

Example

The following example configures an event identified as index 10, for which the device generates a notification in the log table.

```
switchxxxxxx(config)# rmon event 10 log
```

19.9 show rmon events

Use the **show rmon events** EXEC mode command to display the RMON event table.

Syntax

show rmon events

Command Mode

EXEC mode

Example

The following example displays the RMON event table.

```
switchxxxxxx# show rmon events

Index   Description    Type     Community   Owner     Last time sent
-----   -----------    ------   ---------   ------    ------------------
1       Errors         Log      router      CLI       Jan 18 2006 23:58:17
2       High           Log                  Manager   Jan 18 2006 23:59:48
        Broadcast      Trap
```

The following table describes significant fields shown in the display:

Field	Description
Index	Unique index that identifies this event.
Description	Comment describing this event.
Type	Type of notification that the device generates about this event. Can have the following values: **none**, **log**, **trap**, **log-trap**. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations.
Community	If an SNMP trap is to be sent, it is sent with the SNMP community string specified by this octet string.
Owner	The entity that configured this event.
Last time sent	The time this entry last generated an event. If this entry has not generated any events, this value is zero.

19.10 show rmon log

Use the **show rmon log** EXEC mode command to display the RMON log table.

Syntax

show rmon log [*event*]

Parameters

event—Specifies the event index. (Range: 0–65535)

Command Mode

EXEC mode

Example

The following example displays event 1 in the RMON log table.

```
switchxxxxxx# show rmon log 1
Maximum table size: 500 (800 after reset)

Event         Description                Time
-----         --------------          -------------------
1             MIB Var.:               Jan 18 2006 23:48:19
              1.3.6.1.2.1.2.2.1.10.
              53, Delta, Rising,
              Actual Val: 800,
              Thres.Set: 100,
              Interval (sec):1
```

19.11 rmon table-size

Use the **rmon table-size** Global Configuration mode command to configure the maximum size of RMON tables. Use the no form of this command to return to the default size.

Syntax

rmon table-size *{**history** entries* | ***log** entries}*

no rmon table-size *{**history** | **log**}*

Parameters

- **history** *entries*—Specifies the maximum number of history table entries. (Range: 20–270)
- **log** *entries*—Specifies the maximum number of log table entries. (Range: 20–100)

Default Configuration

The default history table size is 270 entries.

The default log table size is 200 entries.

Command Mode

Global Configuration mode

User Guidelines

The configured table size takes effect after the device is rebooted.

Example

The following example configures the maximum size of RMON history tables to 100 entries.

```
switchxxxxxx(config)# rmon table-size history 100
```

20 802.1x Commands

20.1 aaa authentication dot1x

Use the **aaa authentication dot1x** Global Configuration mode command to specify how ports are authenticated when 802.1x is enabled. You can select either authentication by a RADIUS server, no authentication, or both methods. Use the **no** form of this command to restore the default configuration.

Syntax

aaa authentication dot1x default *method1* [*method2*]

no aaa authentication dot1x default

Parameters

method1 [method2]—Specify at least one method from the following:

- **radius** - Uses the list of all RADIUS servers for authentication
- **none** - Uses no authentication

Default Configuration

The default method is RADIUS.

Command Mode

Global Configuration mode

User Guidelines

You can select either authentication by a RADIUS server, no authentication (**none**), or both methods.

If you require that authentication succeeds even if the RADIUS server is not found or returns an error, specify **none** as the final method in the command line.

Example

The following example sets the 802.1X authentication mode to RADIUS server authentication. If no response is received, no authentication is performed.

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

20.2 dot1x system-auth-control

Use the **dot1x system-auth-control** Global Configuration mode command to enable 802.1x globally. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Parameters
N/A

Default Configuration
Disabled.

Command Mode
Global Configuration mode

Example
The following example enables 802.1x globally.

```
switchxxxxxx(config)# dot1x system-auth-control
```

20.3 dot1x port-control
Use the **dot1x port-control** Interface Configuration (Ethernet) mode command to enable manual control of the port authorization state. Use the **no** form of this command to restore the default configuration.

Syntax
dot1x port-control *{**auto** | **force-authorized** | **force-unauthorized**}**[time-range** time-range-name]*

no dot1x port-control

Parameters
- **auto**—Enables 802.1x authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1x authentication exchange between the device and the client.
- **force-authorized**—Disables 802.1x authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port resends and receives normal traffic without 802.1x-based client authentication.
- **force-unauthorized**—Denies all access through this port by forcing it to transition to the unauthorized state and ignoring all attempts by the client to authenticate. The device cannot provide authentication services to the client through this port.
- **time-range** time-range-name—Specifies a time range. When the Time Range is not in effect, the port state is Unauthorized. (Range: 1–32 characters)

Default Configuration
The port is in the force-authorized state.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1x edge ports (ports in **auto** state that are connected to end stations), in order to proceed to the forwarding state immediately after successful authentication.

Example

The following example sets 802.1x authentication on fe1/0/115 to auto mode.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x port-control auto
```

20.4 dot1x reauthentication

Use the **dot1x reauthentication** Interface Configuration mode command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

Syntax

dot1x reauthentication

no dot1x reauthentication

Parameters

N/A

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface configuration (Ethernet)

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# dot1x reauthentication
```

20.5 dot1x timeout reauth-period

Use the **dot1x timeout reauth-period** Interface Configuration mode command to set the number of seconds between re-authentication attempts. Use the **no** form of this command to return to the default setting.

Syntax

dot1x timeout reauth-period *seconds*

no dot1x timeout reauth-period

Parameters

reauth-period *seconds*—Number of seconds between re-authentication attempts. (Range: 300-4294967295)

Default Configuration

3600

Command Mode
Interface Configuration (Ethernet) mode

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

20.6 dot1x re-authenticate

The **dot1x re-authenticate** Privileged EXEC mode command manually initiates re-authentication of all 802.1x-enabled ports or the specified 802.1x-enabled port.

Syntax
dot1x re-authenticate *[interface-id]*

Parameters
interface-id—Specifies an Ethernet port ID.

Default Configuration
If no port is specified, command is applied to all ports.

Command Mode
Privileged EXEC mode

Example
The following command manually initiates re-authentication of 802.1x-enabled fe1/0/115.

```
switchxxxxxx# dot1x re-authenticate fe1/0/115
```

20.7 dot1x timeout quiet-period

Use the **dot1x timeout quiet-period** Interface Configuration (Ethernet) mode command to set the time interval that the device remains in a quiet state following a failed authentication exchange (for example, the client provided an invalid password). Use the **no** form of this command to restore the default configuration.

Syntax
dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameters
seconds—Specifies the time interval in seconds that the device remains in a quiet state following a failed authentication exchange with the client. (Range: 0–65535 seconds)

Default Configuration
The default quiet period is 60 seconds.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
During the quiet period, the device does not accept or initiate authentication requests.

The default value of this command should only be changed to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To provide faster response time to the user, a smaller number than the default value should be entered.

Example
The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 10 seconds.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x timeout quiet-period 10
```

20.8 dot1x timeout tx-period
Use the **dot1x timeout tx-period** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

Syntax
dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Parameters
seconds—Specifies the time interval in seconds during which the device waits for a response to an EAP-request/identity frame from the client before resending the request. (Range: 30–65535 seconds)

Default Configuration
The default timeout period is 30 seconds.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example
The following command sets the time interval during which the device waits for a response to an EAP request/identity frame to 60 seconds.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

20.9 dot1x max-req

Use the **dot1x max-req** Interface Configuration mode command to set the maximum number of times that the device sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

max-req *count*—Specifies the maximum number of times that the device sends an EAP request/identity frame before restarting the authentication process. (Range: 1–10)

Default Configuration

The default maximum number of attempts is 2.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the maximum number of times that the device sends an EAP request/identity frame to 6

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x max-req 6
```

20.10 dot1x timeout supp-timeout

Use the **dot1x timeout supp-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response to an Extensible Authentication Protocol (EAP) request frame from the client before resending the request. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameters

supp-timeout *seconds*—Specifies the time interval in seconds during which the device waits for a response to an EAP request frame from the client before resending the request. (Range: 1–65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the time interval during which the device waits for a response to an EAP request frame from the client before resending the request to 3600 seconds.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

20.11 dot1x timeout server-timeout

Use the **dot1x timeout server-timeout** Interface Configuration (Ethernet) mode command to set the time interval during which the device waits for a response from the authentication server. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Parameters

server-timeout *seconds*—Specifies the time interval in seconds during which the device waits for a response from the authentication server. (Range: 1–65535 seconds)

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The actual timeout period can be determined by comparing the value specified by the **dot1x timeout server-timeout** command to the result of multiplying the number of retries specified by the radius-server retransmit command by the timeout period specified by the radius-server retransmit command, and selecting the lower of the two values.

Example
The following example sets the time interval between retransmission of packets to the authentication server to 3600 seconds.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

20.12 show dot1x
Use the **show dot1x** Privileged EXEC mode command to display the 802.1x device or specified interface status.

Syntax
show dot1x ***[interface*** *interface-id]*

Parameters
interface-id—Specify an Ethernet port ID.

Default Configuration
Display for all ports.

Command Mode
Privileged EXEC mode

Examples

Example 1 - The following example displays the status of a single 802.1x-enabled Ethernet ports.

```
switchxxxxxx# show dot1x interface fe1/0/13
802.1x is enabled.

Port        Admin        Oper           Reauth     Reauth   Username
            Mode         Mode           Control    Period
----        ----------   ------------   -------    ------   --------
fe1/0/1     Auto         Unauthorized   Ena        3600     Clark
3

Time-range:             work-hours (Inactive now)
Quiet period:           60 Seconds
Tx period:              30 Seconds
Max req:                2
Supplicant timeout:     30 Seconds

Server timeout:                         30 Seconds
Session Time (HH:MM:SS):                08:19:17
MAC Address:                            00:08:78:32:98:78
Authentication Method:                  Remote
Termination Cause:                      Supplicant logoff

Authenticator State Machine

State:                                  HELD

Backend State Machine

State:                                  IDLE
Authentication success:                 9
Authentication fails:                   1
```

Example 2 - The following example displays the status of all 802.1x-enabled Ethernet ports.

```
switchxxxxxx# show dot1x
802.1x is enabled

Port        Admin        Oper           Reauth     Reauth   Username
            Mode         Mode           Control    Period
----        ----------   ------------   -------    ------   --------
fe1/0/1     Auto         Authorized     Ena        3600     Bob
1           Auto         Authorized     Ena        3600     John
fe1/0/1     Auto         Unauthorized   Ena        3600     Clark
2           Force-auth   Authorized     Dis        3600     n/a
fe1/0/1     Force-auth   Unauthorized   Dis        3600     n/a
3
fe1/0/1
4
fe1/0/1
5

* Port is down or not present.
```

The following table describes the significant fields shown in the display.

Field	Description
Port	The port number.
Admin mode	The port administration (configured) mode. Possible values: Force-auth, Force-unauth, Auto.
Oper mode	The port operational (actual) mode. Possible values: Authorized, Unauthorized or Down.
Reauth Control	Reauthentication control.
Reauth Period	Reauthentication period.
Username	Username representing the supplicant identity. This field shows the username if the port control is auto. If the port is Authorized, it displays the username of the current user. If the port is Unauthorized, it displays the last user authenticated successfully.
Quiet period	Number of seconds that the device remains in the quiet state following a failed authentication exchange (for example, the client provided an invalid password).
Tx period	Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the client before resending the request.
Max req	Maximum number of times that the device sends an EAP request frame (assuming that no response is received) to the client before restarting the authentication process.
Supplicant timeout	Number of seconds that the device waits for a response to an EAP-request frame from the client before resending the request.
Server timeout	Number of seconds that the device waits for a response from the authentication server before resending the request.
Session Time	Amount of time (HH:MM:SS) that the user is logged in.
MAC address	Supplicant MAC address.
Authentication Method	Authentication method used to establish the session.
Termination Cause	Reason for the session termination.
State	Current value of the Authenticator PAE state machine and of the Backend state machine.
Authentication success	Number of times the state machine received a Success message from the Authentication Server.
Authentication fails	Number of times the state machine received a Failure message from the Authentication Server.

20.13 show dot1x users

Use the **show dot1x users** Privileged EXEC mode command to display active 802.1x authenticated users for the device.

Syntax
show dot1x users *[**username** username]*

Parameters
username—Specifies the supplicant username (Length: 1–160 characters)

Default Configuration
Display all users.

Command Mode
Privileged EXEC mode

Example
The following example displays 802.1x user with supplicant username Bob.

```
switchxxxxxx# show dot1x users username Bob
Port    Username     Session        Auth       MAC             VLAN
                     Time           Method     Address
--------- ------------------------------  -----------      ----
fe1/0/11 Bob       1d 09:07:38    Remote     0008.3b79.8787    3
```

20.14 show dot1x statistics
Use the **show dot1x statistics** Privileged EXEC mode command to display 802.1x statistics for the specified port.

Syntax
show dot1x statistics interface *interface-id*

Parameters
interface-id—Specifies an Ethernet port ID.

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays 802.1x statistics for `fe1/0/11`.

```
switchxxxxxx# show dot1x statistics interface fe1/0/11
EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
```

```
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:08:78:32:98:78
```

The following table describes the significant fields shown in the display:

Field	Description
EapolFramesRx	Number of valid EAPOL frames of any type that have been received by this Authenticator.
EapolFramesTx	Number of EAPOL frames of any type that have been transmitted by this Authenticator.
EapolStartFramesRx	Number of EAPOL Start frames that have been received by this Authenticator.
EapolLogoffFramesRx	Number of EAPOL Logoff frames that have been received by this Authenticator.
EapolRespIdFramesRx	Number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	Number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
EapolReqIdFramesTx	Number of EAP Req/Id frames that have been transmitted by this Authenticator.
EapolReqFramesTx	Number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Authenticator.
InvalidEapolFramesRx	Number of EAPOL frames that have been received by this Authenticator for which the frame type is not recognized.
EapLengthErrorFramesRx	Number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	Protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Source MAC address carried in the most recently received EAPOL frame.

20.15 clear dot1x statistics

Use the **clear dot1x statistics** Privileged EXEC mode command to clear 802.1x statistics.

Syntax

clear dot1x statistics [*interface-id*]

Parameters
interface-id—Specify an Ethernet port ID.

Default Configuration
Statistics on all ports are cleared.

Command Mode
Privileged EXEC

User Guidelines
The command clears the statistics displayed in the show dot1x statistics command

Example

```
switchxxxxxx# clear dot1x statistics
```

20.16 dot1x host-mode
Use the **dot1x host-mode** Interface Configuration mode command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

Syntax
dot1x host-mode ***{multi-host*** | ***single-host*** | ***multi-sessions}***

Parameters
- **multi-host**—Enable multiple-hosts mode.
- **single-host**—Enable single-hosts mode.
- **multi-sessions**—Enable multiple-sessions mode.

Default Configuration
Default mode is multi-host.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
In multiple hosts mode only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized, all attached clients are denied access to the network.

In multiple sessions mode each host must be successfully authorized in order to grant network access. Please note that packets are NOT encrypted, and after success full authentication filtering is based on the source MAC address only.

Port security on a port cannot be enabled in single-host mode and in multiple-sessions mode.

It is recommended to enable reauthentication when working in multiple-sessions mode in order to detect user logout for users that have not logged off.

In single host mode there is only one attached host and only this authenticated host can access the network.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# dot1x host-mode multi-host
switchxxxxxx(config-if)# dot1x host-mode single-host
switchxxxxxx(config-if)# dot1x host-mode multi-sessions
```

20.17 dot1x violation-mode

Use the **dot1x violation-mode** Interface Configuration (Ethernet) mode command to configure the action to be taken, when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. Use the **no** form of this command to return to default.

Syntax

dot1x violation-mode ***{restrict*** | ***protect*** | ***shutdown}*** **no dot1x violation-mode**

Parameters

- **restrict**—Generates a trap when a station whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. Those frames are forwarded but their source address are not learned.
- **protect**—Discard frames with source addresses not the supplicant address.
- **shutdown**—Discard frames with source addresses not the supplicant address and shutdown the port

Default Configuration

Protect

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The command is relevant only for single-host mode.

BPDU message whose MAC address is not the supplicant MAC address wouldn't be discarded in the protect mode.

BPDU message whose MAC address is not the supplicant MAC address would cause a shutdown in the shutdown mode.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# dot1x violation-mode protect
```

20.18 dot1x guest-vlan

Use the **dot1x guest-vlan** Interface Configuration (VLAN) mode command to define a guest VLAN. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Parameters

N/A

Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Use the **dot1x guest-vlan enable** Interface Configuration mode command to enable unauthorized users on an interface to access the guest VLAN.

If the guest VLAN is defined and enabled, the port automatically joins the guest VLAN when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave the guest VLAN, the port should not be a static member of the guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# dot1x guest-vlan
```

20.19 dot1x guest-vlan timeout

Use the **dot1x guest-vlan timeout** Global Configuration mode command to set the time delay between enabling 802.1x (or port up) and adding a port to the guest VLAN. Use the **no** form of this command to restore the default configuration.

Syntax

dot1x guest-vlan timeout *timeout*

no dot1x guest-vlan timeout

Parameters

timeout—Specifies the time delay in seconds between enabling 802.1x (or port up) and adding the port to the guest VLAN. (Range: 30–180)

Default Configuration

The guest VLAN is applied immediately.

Command Mode
Global Configuration mode

User Guidelines
This command is relevant if the guest VLAN is enabled on the port. Configuring the timeout adds delay from enabling 802.1X (or port up) to the time the device adds the port to the guest VLAN.

Example
The following example sets the delay between enabling 802.1x and adding a port to a guest VLAN to 60 seconds.

```
switchxxxxxx(config)# dot1x guest-vlan timeout 60
```

20.20 dot1x guest-vlan enable
Use the **dot1x guest-vlan enable** Interface Configuration (Ethernet) mode command to enable unauthorized users on the interface access to the guest VLAN. Use the **no** form of this command to disable access.

Syntax
dot1x guest-vlan enable

no dot1x guest-vlan enable

Parameters
N/A

Default Configuration
The default configuration is disabled.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
A device can have only one global guest VLAN. The guest VLAN is defined using the dot1x guest-vlan Interface Configuration mode command.

Example
The following example enables unauthorized users on fe1/0/11 to access the guest VLAN.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

20.21 dot1x mac-authentication
Use the **dot1x mac-authentication** Interface Configuration (Ethernet) mode command to enable authentication based on the station's MAC address. Use the **no** form of this command to disable this feature.

Syntax

dot1x mac-authentication {***mac-only*** | ***mac-and-802.1x***}

no dot1x mac-authentication

Parameters

- **mac-only**—Enables authentication based on the station's MAC address only. 802.1X frames are ignored.
- **mac-and-802.1x**—Enables 802.1X authentication and MAC address authentication on the interface.

Default Configuration

Authentication based on the station's MAC address is disabled.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

The guest VLAN must be enabled when MAC authentication is enabled.

Static MAC addresses cannot be authorized. Do not change an authenticated MAC address to a static address.

It is not recommended to delete authenticated MAC addresses.

Reauthentication must be enabled when working in this mode.

Example

The following example enables authentication based on the station's MAC address on `fe1/0/11`.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# dot1x mac-authentication mac-only
```

20.22 dot1x traps mac-authentication success

Use the **dot1x traps mac-authentication success** Global Configuration mode command to enable sending traps when a MAC address is successfully authenticated by the 802.1X MAC-authentication access control. Use the **no** form of this command to disable the traps.

Syntax

dot1x traps mac-authentication success

no dot1x traps mac-authentication success

Parameters

N/A

Default Configuration

Default is disabled.

Command Mode
Global Configuration mode

Example
The following example enables sending traps when a MAC address is successfully authenticated by the 802.1X MAC-authentication access control.

```
switchxxxxxx(config-if)# dot1x traps mac-authentication success
```

20.23 dot1x traps mac-authentication failure

Use the **dot1x traps mac-authentication failure** Global Configuration mode command to enable sending traps when MAC address was failed in authentication of the 802.1X MAC authentication access control. Use the **no** form of this command to disable the traps.

Syntax
dot1x traps mac-authentication failure

no dot1x traps mac-authentication failure

Parameters
N/A

Default Configuration
Default is Enabled.

Command Mode
Global Configuration mode

Example
The following example enables sending traps when a MAC address fails to be authenticated by the 802.1X mac-authentication access control.

```
switchxxxxxx(config-if)# dot1x traps mac-authentication failure
```

20.24 dot1x radius-attributes vlan

Use the **dot1x radius-attributes vlan** Interface Configuration mode command, to enable user-based VLAN assignment. Use the **no** form of this command to disable user-based VLAN assignment.

Syntax
dot1x radius-attributes vlan

no dot1x radius-attributes vlan

Parameters
N/A

Default Configuration
Disabled

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
The configuration of this command is allowed only when the port is Forced Authorized.

RADIUS attributes are supported only in the multiple sessions mode (multiple hosts with authentication)

When RADIUS attributes are enabled and the RADIUS Accept message does not contain the supplicant's VLAN as an attribute, then the supplicant is rejected.

Packets to the supplicant are sent untagged.

After successful authentication, the port remains a member in the unauthenticated VLANs and in the Guest VLAN. Other static VLAN configuration is not applied on the port. If the supplicant VLAN does not exist on the switch, the supplicant is rejected.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# dot1x radius-attributes vlan
```

20.25 dot1x radius-attributes filter-id

Use the **dot1x radius-attributes filter-id** Interface Configuration mode command to enable user-based ACL/Qos-Policy assignment. Use the **no** form of this command to disable user-based ACL/Qos-Policy assignment.

Syntax
dot1x radius-attributes filter-id

no dot1x radius-attributes filter-id

Parameters
N/A

Default Configuration
Disabled

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
User based ACL/Qos-Policy assignment is supported only in 802.1x multiple sessions.

The configuration of the parameter is allowed only when the port is Forced Authorized or Forced Unauthorized.

Example
The following example enables user-based ACL/Qos-Policy assignment.

```
switchxxxxxx(config-if)# dot1x radius-attributes filter-id
```

20.26 dot1x radius-attributes errors
Use the **dot1x radius-attributes errors** Global Configuration mode command to specify error handling for the RADIUS attributes feature. Use the **no** form of this command to return to the default.

Syntax
dot1x radius-attributes errors filter-id resources *{**accept** | **reject**}*

no dot1x radius-attributes errors filter-id resources

Parameters
- **accept**—If the Filter-ID cannot be allocated for resource allocation reasons, the user is accepted. If the Filter-ID canot be allocated for other reasons, the user is rejected.
- **reject**—If the Filter-ID cannot be assigned, the user is rejected.

Default Configuration
Reject

Command Mode
Global Configuration mode

Example
The following example accepts users who cannot be allocated.

```
switchxxxxxx(config-if)# dot1x radius-attributes errors filter-id resources accept
```

20.27 show dot1x advanced
Use the **show dot1x advanced** Privileged EXEC mode command to display 802.1x advanced features for the device or specified interface.

Syntax
show dot1x advanced *[interface-id]*

Parameters
nterface-id—Specify an Ethernet port ID.

Command Mode
Privileged EXEC mode

Example

The following example displays 802.1x advanced features for the device.

```
switchxxxxxx# show dot1x advanced
Guest VLAN: 3978
Guest VLAN Timeout:
Unauthenticated VLANs: 91, 92
Interface Multiple Guest   MAC             VLAN        Legacy-  Policy
          Hosts    VLAN    Authentication  Assignment  supp Mode  Assignment
------- ---------- ------ ---------------- ----------  --------- ----------
fe1/0/11   Disabled Enabled MAC-and-802.1X  Enabled     Enable      Disabled
fe1/0/12   Enabled  Disabled Disabled       Enabled     Enable      Disabled
```

```
switchxxxxxx# show dot1x advanced fe1/0/11
Interface Multiple Guest   MAC              VLAN        Legacy-  Policy
          Hosts    VLAN    Authentication   Assignment sup Mode Assignment
------------------ ----------------------  ----------  ------  ----------
fe1/0/11   Disabled Enabled  MAC-and-802.1X    Enabled     Enable
Legacy-Supp mode is disabled
Policy assignment resource err handling: Accept
Single host parameters
Violation action: Discard
Trap: Enabledx
Status: Single-host locked
Violations since last trap: 9
```

21 Ethernet Configuration Commands

21.1 interface

Use the **interface** Global Configuration mode command to enter Interface configuration mode in order to configure an interface.

Syntax

interface *interface-id*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel, VLAN, range, IP interface or tunnel.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, Port-channel, VLAN, range, IP interface or tunnel) mode

Examples

Example 1 - For Gigabit Ethernet ports:

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)#
```

Example 2 - For Fast Ethernet ports:

```
switchxxxxxx(config)# interface fa1
switchxxxxxx(config-if)#
```

Example 3 - For port channels (LAGs):

```
switchxxxxxx(config)# interface po1
switchxxxxxx(config-if)#
```

21.2 interface range

Use the **interface range** command to execute a command on multiple ports at the same time.

Syntax

interface range *interface-id-list*

Parameters
interface-id-list—Specify list of interface IDs. The interface ID can be one of the following types: Ethernet port, VLAN, or Port-channel

Default Configuration
N/A

Command Mode
Interface Configuration (Ethernet, Port-channel, or VLAN) mode

User Guidelines
Commands under the interface range context are executed independently on each interface in the range: If the command returns an error on one of the interfaces, it does not stop the execution of the command on other interfaces.

Example

```
switchxxxxxx(config)# interface range fe1/0/11-20
switchxxxxxx(config-if-range)#
```

21.3 shutdown
Use the **shutdown** Interface Configuration (Ethernet, Port-channel) mode command to disable an interface. Use the **no** form of this command to restart a disabled interface.

Syntax
shutdown

no shutdown

Parameters
N/A

Default Configuration
The interface is enabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
Example 1 - The following example disables `fe1/0/15` operations.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 2 - The following example restarts the disabled Ethernet port.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# no shutdown
switchxxxxxx(config-if)
```

21.4 description

Use the **description** Interface Configuration (Ethernet, Port-channel) mode command to add a description to an interface. Use the **no** form of this command to remove the description.

Syntax

description *string*

no description

Parameters

string—Specifies a comment or a description of the port to assist the user. (Length: 1–64 characters).

Default Configuration

The interface does not have a description.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example adds the description 'SW#3' to `fe1/0/1`5.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# description SW#3
```

21.5 speed

Use the **speed** Interface Configuration (Ethernet, Port-channel) mode command to configure the speed of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default configuration.

Syntax

speed *{10 | 100 | 1000}*

no speed

Parameters

- **10**—Forces10 Mbps operation.
- **100**—Forces 100 Mbps operation.
- **1000**—Forces 1000 Mbps operation.

Default Configuration
The port operates at its maximum speed capability.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
The **no speed** command in a port-channel context returns each port in the port-channel to its maximum capability.

Example
The following example configures the speed of `fe1/0/15` to 100 Mbps operation.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# speed 100
```

21.6 duplex
Use the **duplex** Interface Configuration (Ethernet, Port-channel) mode command to configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation. Use the **no** form of this command to restore the default configuration.

Syntax
duplex ***{half | full}***

no duplex

Parameters
- **half**—Forces half-duplex operation.
- **full**—Forces full-duplex operation.

Default Configuration
The interface operates in full duplex mode.

Command Mode
Interface Configuration (Port-channel) mode

Example
The following example configures `fe1/0/15` to operate in full duplex mode.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# duplex full
```

21.7 negotiation
Use the **negotiation** Interface Configuration (Ethernet, Port-channel) mode command to enable auto-negotiation operation for the speed and duplex parameters of a given interface. Use the **no** form of this command to disable auto-negotiation.

Syntax

negotiation [*capability* [*capability2... capability5*]]

no negotiation

Parameters

capability—Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f).

- **10h** - Advertise 10 half-duplex
- **10f** - Advertise 10 full-duplex
- **100h** - Advertise 100 half-duplex
- **100f** - Advertise 100 full-duplex
- **1000f** - Advertise 1000 full-duplex

Default Configuration

If capability is unspecified, defaults to list of all the capabilities of the port.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example enables auto-negotiation on `fe1/0/15`.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# negotiation
```

21.8 flowcontrol

Use the **flowcontrol** Interface Configuration (Ethernet, Port-channel) mode command to configure the flow control on a given interface. Use the **no** form of this command to disable flow control.

Syntax

flowcontrol ***{auto*** | ***on*** | ***off}***

no flowcontrol

Parameters

- **auto**—Specifies auto-negotiation of flow control.
- **on**—Enables flow control.
- **off**—Disables flow control.

Default Configuration

Flow control is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Use the **negotiation** command to enable **flow control auto**.

Example
The following example enables flow control on port `fe1/0/11`

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# flowcontrol on
```

21.9 mdix
Use the **mdix** Interface Configuration (Ethernet) mode command to enable cable crossover on a given interface. Use the **no** form of this command to disable cable crossover.

Syntax
mdix ***{on*** | ***auto}***

no mdix

Parameters
- **on**—Enables manual MDIX.
- **auto**—Enables automatic MDI/MDIX.

Default Configuration
The default setting is On.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example enables automatic crossover on port `fe1/0/15`.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# mdix auto
```

21.10 back-pressure
Use the **back-pressure** Interface Configuration (Ethernet) mode command to enable back pressure on a specific interface. Use the **no** form of this command to disable back pressure.

Syntax
back-pressure

no back-pressure

Default Configuration
Back pressure is disabled.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
Back-pressure cannot be enabled when EEE is enabled.

Example
The following example enables back pressure on port `fe1/0/15`.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# back-pressure
```

21.11 port jumbo-frame
Use the **port jumbo-frame** Global Configuration mode command to enable jumbo frames on the device. Use the **no** form of this command to disable jumbo frames.

Syntax
port jumbo-frame

no port jumbo-frame

Default Configuration
Jumbo frames are disabled on the device.

Command Mode
Global Configuration mode

User Guidelines
This command takes effect only after resetting the device.

Example
The following example enables jumbo frames on the device.

```
switchxxxxxx(config)# port jumbo-frame
```

21.12 clear counters
Use the **clear counters** EXEC mode command to clear counters on all or on a specific interface.

Syntax
clear counters *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
All counters are cleared.

Command Mode
EXEC mode

Example
The following example clears the statistics counters for `fe1/0/15`.

```
switchxxxxxx# clear counters fe1/0/15.
```

21.13 set interface active
Use the **set interface active** EXEC mode command to reactivate an interface that was shut down.

Syntax
set interface active *{interface-id}*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

User Guidelines
This command is used to activate interfaces that were configured to be active, but were shut down by the system.

Example
The following example reactivates `fe1/0/11`.

```
switchxxxxxx# set interface active fe1/0/11
```

21.14 errdisable recovery cause
Use the **errdisable recovery cause** Global Configuration mode command to enable automatic re-activation of an interface after Err-Disable shutdown. Use the **no** form of this command to disable automatic re-activation.

Syntax
errdisable recovery cause *{all | port-security | dot1x-src-address | acl-deny |stp-bpdu-guard | stp-loopback-guard}*

no errdisable recovery cause *{all | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard}*

Parameters
all - Enables the error recovery mechanism for all the reasons

port-security - Enables the error recovery mechanism for the port security Err-Disable state.

dot1x-src-address - Enables the error recovery mechanism for the 802.1x Err-Disable state.

acl-deny - Enables the error recovery mechanism for the ACL Deny Err-Disable state.

stp-bpdu-guard - Enables the error recovery mechanism for thee STP BPDU Guard Err-Disable state.

stp-loopback-guard - Enables the error recovery mechanism for the STP Loopback Guard Err-Disable state.

Default Configuration
Automatic re-activation is disabled.

Command Mode
Global Configuration mode

Example
The following example enables automatic re-activation of an interface after Loopback Detection Err-Disable shutdown.

```
switchxxxxxx(config)# errdisable recovery cause loopback-detection
```

21.15 errdisable recovery interval

Use the **errdisable recovery interval** Global Configuration mode command timeout interval to set the error recovery timeout interval. Use the **no** form of this command to return to the default configuration.

Syntax
errdisable recovery interval *seconds*

no errdisable recovery interval

Parameters
seconds—Specifies the error recovery timeout interval in seconds. (Range: 30–86400)

Default Configuration
The default error recovery timeout interval is 300 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the error recovery timeout interval to 10 minutes.

```
switchxxxxxx(config)# errdisable recovery interval 600
```

21.16 show interfaces configuration

Use the **show interfaces configuration** EXEC mode command to display the configuration for all configured interfaces or for a specific interface.

Syntax

show interfaces configuration *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display all

Command Mode

EXEC mode

Example

The following example displays the configuration of all configured interfaces:

```
switchxxxxxx# show interfaces configuration
                                                Flow      Admin  Back       Mdix
Port    Type       Duplex  Speed  Neg      control   State  Pressure   Mode
------ --------- ------  -----  -------- -------   -----  --------   ----
fe1/0/11    1G-Copper Full    10000  Disabled Off       Up     Disabled   Off
fe1/0/12    1G-Copper Full    1000   Disabled Off       Up     Disabled   Off
                                      Flow      Admin
PO      Type    Speed  Neg        Control   State
------  ------ -----  --------   -------   -----
Po1                    Disabled   Off       Up
```

21.17 show interfaces status

Use the **show interfaces status** EXEC mode command to display the status of all interfaces or of a specific interface.

Syntax

show interfaces status *[interface-id] [**detailed**]*

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detailed**—Displays information for non-present ports in addition to present ports.

Command Mode

EXEC mode

Default Configuration
Display for all interfaces.

Example
The following example displays the status of all configured interfaces.

```
switchxxxxxx# show interfaces status
                                        Flow  Link   Back     Mdix
Port   Type      Duplex Speed Neg       ctrl  State  Pressure Mode
------ --------- ------ ----- -------- ----  ------ -------- --
fe1/0/11    1G-Copper Full   1000  Disabled Off   Up     Disabled Off
fe1/0/12    1G-Copper --     --     --       --    Down   --       --
                                        Flow     Link
PO     Type      Duplex Speed  Neg     control  State
-----  -------   ------ -----  ------- ----     ------
Po1    1G        Full   10000  Disabled Off     Up
```

21.18 show interfaces advertise
Use the **show interfaces advertise** EXEC mode command to display auto-negotiation advertisement information for all configured interfaces or for a specific interface.

Syntax
show interfaces advertise *[interface-id* |

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
Display for all interfaces.

Command Mode
EXEC mode

Examples
The following examples display auto-negotiation information.

```
switchxxxxxx# show interfaces advertise
Port       Type         Neg       Operational Link Advertisement
----       ---------    ------    ------------------------------
fe1/0/11   1G-Copper    Enable    1000f, 100f, 10f, 10h
fe1/0/12   1G-Copper    Enable    1000f
```

```
switchxxxxxx# show interfaces advertise fe1/0/11
Port:fe1/0/11
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
                                  10h   10f   100h   100f   1000f
                                  ---   ---   ----   ----   -----
Admin Local link Advertisement    yes   yes   yes    yes    yes
Oper Local link Advertisement     yes   yes   yes    yes    yes
Remote Local link                 no    no    yes    yes    yes
Advertisement                     -     -     -      -      yes
Priority Resolution
```

```
switchxxxxxx# show interfaces advertise fe1/0/11
Port: fe1/0/11
Type: 1G-Copper
Link state: Up
Auto negotiation: disabled.
```

21.19 show interfaces description

Use the **show interfaces description** EXEC mode command to display the description for all configured interfaces or for a specific interface.

Syntax

show interfaces description *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display description for all interfaces.

Command Mode

EXEC mode

Example

The following example displays the description of all configured interfaces.

```
switchxxxxxx# show interfaces description
```

```
Port        Descriptions
fe1/0/11    ---------------------------------------------
fe1/0/12    Port that should be used for management only
fe1/0/13
fe1/0/14

PO          Description
----        -----------
Po1         Output
```

21.20 show interfaces counters

Use the **show interfaces counters** EXEC mode command to display traffic seen by all the physical interfaces or by a specific interface.

Syntax

show interfaces counters *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display counters for all interfaces.

Command Mode

EXEC mode

Example

The following example displays traffic seen by all the physical interfaces.

```
switchxxxxxx# show interfaces counters fe1/0/11
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
fe1/0/11           0            0            0            0
Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
fe1/0/11           0            1            35          7051
Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
```

```
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

The following table describes the fields shown in the display.

Field	Description
InOctets	Number of received octets.
InUcastPkts	Number of received unicast packets.
InMcastPkts	Number of received multicast packets.
InBcastPkts	Number of received broadcast packets.
OutOctets	Number of transmitted octets.
OutUcastPkts	Number of transmitted unicast packets.
OutMcastPkts	Nmber of transmitted multicast packets.
OutBcastPkts	Number of transmitted broadcast packets.
FCS Errors	Number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	Number of frames that are involved in a single collision, and are subsequently transmitted successfully.
Multiple Collision Frames	Number of frames that are involved in more than one collision and are subsequently transmitted successfully.
SQE Test Errors	Number of times that the SQE TEST ERROR is received. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6.
Deferred Transmissions	Number of frames for which the first transmission attempt is delayed because the medium is busy.
Late Collisions	Number of times that a collision is detected later than one slotTime into the transmission of a packet.
Excessive Collisions	Number of frames for which transmission fails due to excessive collisions.
Oversize Packets	Number of frames received that exceed the maximum permitted frame size.
Internal MAC Rx Errors	Number of frames for which reception fails due to an internal MAC sublayer receive error.
Received Pause Frames	Number of MAC Control frames received with an opcode indicating the PAUSE operation.
Transmitted Pause Frames	Number of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation.

21.21 show ports jumbo-frame

Use the **show ports jumbo-frame** EXEC mode command to display the whether jumbo frames are enabled on the device.

Syntax

show port jumbo-frame

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays whether jumbo frames are enabled on the device.

```
switchxxxxxx# show ports jumbo-frame
Jumbo frames are disabled
Jumbo frames will be enabled after reset
```

21.22 show errdisable recovery

Use the **show errdisable recovery** EXEC mode command to display the Err-Disable configuration of the device.

Syntax

show errdisable recovery

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays the Err-Disable configuration.

```
switchxxxxxx# show errdisable recovery
Timer interval: 300 Seconds
```

```
        Reason          Automatic Recovery
---------------------- ------------------
port-security          Disable
dot1x-src-address      Disable
acl-deny               Enable
stp-bpdu-guard         Disable
stp-loopback-guard     Disable
```

21.23 show errdisable interfaces

Use the **show errdisable interfaces** EXEC mode command to display the Err-Disable state of all interfaces or of a specific interface.

Syntax

show errdisable interfaces *[interface-id]*

Parameters

- **interface**—Interface number
- **port-channel-number**—Port channel index.

Default Configuration

Display for all interfaces.

Command Mode

EXEC mode

Example

The following example displays the Err-Disable state of all interfaces.

```
switchxxxxxx# show errdisable interfaces
Interface        Reason                    Automatic Recovery
---------        ------------------        -------------------
fe1/0/11              port-security             No
fe1/0/112           acl-deny                  Yes
```

21.24 storm-control broadcast enable

Use the **storm-control broadcast enable** Interface Configuration mode command to enable storm control on a port. Use the **no** form of this command to disable storm control.

Syntax

storm-control broadcast enable

no storm-control broadcast enable

Parameters
This command has no arguments or keywords.

Default Configuration
Disabled

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Use the storm-control include-multicast Interface Configuration command to count Multicast packets and optionally unknown Unicast packets in the storm control calculation.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# storm-control broadcast enable
```

21.25 storm-control broadcast level kbps
Use the **storm-control broadcast level** Interface Configuration mode command to configure the maximum rate of broadcast on a port. Use the **no** form of this command to return to default.

Syntax
storm-control broadcast level kbps *kbps*

no storm-control broadcast level

Parameters

3500-10G

Default Configuration
1000

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
Use the **storm-control broadcast enable** Interface Configuration command to enable storm control.

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# storm-control broadcast level kbps 12345
```

21.26 storm-control include-multicast

Use the **storm-control include-multicast** Interface Configuration mode command to count Multicast packets in a Broadcast storm control. Use the **no** form of this command to disable counting of Multicast packets in the Broadcast storm control.

Syntax

storm-control include-multicast ***[unknown-unicast]***

no storm-control include-multicast

Parameters

unknown-unicast—Specifies also the count of unknown unicast packets.

Default Configuration

Disabled

Command Mode

Interface Configuration mode (Ethernet)

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# storm-control include-multicast
```

22 PHY Diagnostics Commands

22.1 test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** Privileged EXEC mode command to use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port.

Syntax

test cable-diagnostics tdr interface *interface-id*

Parameters

interface-id—Specifies an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The port to be tested should be shut down during the test, unless it is a combination port with fiber port active.

The maximum length of cable for the TDR test is 120 meters.

Example

The following examples test the copper cables attached to ports 7 and 8.

```
switchxxxxxx# test cable-diagnostics tdr interface fe1/0/17
Cable is open at 64 meters
switchxxxxxx# test cable-diagnostics tdr interface fe1/0/18
Can't perform the test on fiber ports
```

22.2 show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** EXEC mode command to display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port.

Syntax

show cable-diagnostics tdr [***interface*** *interface-id*]

Parameters

interface-id—Specifies an Ethernet port ID.

Default Configuration

All ports are displayed.

Command Mode
EXEC mode

User Guidelines
The maximum length of cable for the TDR test is 120 meters.

Example
The following example displays information on the last TDR test performed on all copper ports.

```
switchxxxxxx# show cable-diagnostics tdr

Port      Result     Length           Date
----      --------   [meters]         ------------------
                     ------------

fe1/0/11  OK
fe1/0/12  Short      50               13:32:00 23 July 2010
fe1/0/13  Test has not been performed
fe1/0/14  Open       64               13:32:00 23 July 2010
fe1/0/15  Fiber      -                -
```

22.3 show cable-diagnostics cable-length

Use the **show cable-diagnostics cable-length** EXEC mode command to display the estimated copper cable length attached to all ports or to a specific port.

Syntax
show cable-diagnostics cable-length [***interface*** *interface-id*]

Parameters
interface-id—Specifies an Ethernet port ID.

Default Configuration
All ports are displayed.

Command Mode
EXEC mode

User Guidelines
The port must be active and working at 100 M or 1000 M.

Example

The following example displays the estimated copper cable length attached to all ports.

```
switchxxxxxx# show cable-diagnostics cable-length
Port           Length [meters]
----           -----------------
fe1/0/11       < 50
fe1/0/12       Copper not active
fe1/0/13       110-140
fe1/0/14       Fiber
```

22.4 show fiber-ports optical-transceiver

Use the **show fiber-ports optical-transceiver** EXEC mode command to display the optical transceiver diagnostics.

Syntax

show fiber-ports optical-transceiver [***interface*** *interface-id*] [***detailed***]

Parameters

- **interface-id**—Specifies an Ethernet port ID.
- **detailed**—Displays detailed diagnostics.

Command Mode

EXEC mode

Example

The following examples display the optical transceiver diagnostics results.

```
switchxxxxxx# show fiber-ports optical-transceiver
   Port      Temp  Voltage Current  Output Input   LOS
                                    Power  Power
----------- ------ ------- -------  ------ -----   ---
   fe1/0/11       W       OK      OK     OK     OK      OK
   fe1/0/12       OK      OK      OK     E      OK      OK
 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported,
 W - Warning, E - Error
```

```
switchxxxxxx# show fiber-ports optical-transceiver detailed
   Port      Temp  Voltage Current Output  Input   LOS
             [C]   [Volt]  [mA]    Power   Power
                                   [mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- ---
  fe1/0/11     Copper
  fe1/0/16     Copper
  fe1/0/17      28    3.32    7.26    3.53    3.68   No
  fe1/0/18      29    3.33    6.50    3.53    3.71   No
 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error
```

23 Green Ethernet

23.1 green-ethernet energy-detect (global)

Use the **green-ethernet energy-detect** Global Configuration mode command to enable Green-Ethernet Energy-Detect mode globally. Use the **no** form of this command to disabled it.

Syntax

green-ethernet energy-detect

no green-ethernet energy-detect

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# green-ethernet energy-detect
```

23.2 green-ethernet energy-detect (interface)

Use the **green-ethernet energy-detect** Interface configuration mode command to enable green-ethernet Energy-Detect mode on a port. Use the no form of this command, to disable it on a port.

Syntax

green-ethernet energy-detect

no green-ethernet energy-detect

Parameters

N/A

Default Configuration

Enabled

Command Mode

Interface configuration mode (Ethernet)

User Guidelines

Energy-Detect can work only when the port is a copper port. When a port is enabled for auto selection, copper/fiber Energy-Detect cannot work.

It takes the PHY ~5 seconds to fall into sleep mode when the link is lost after normal operation.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# green-ethernet energy-detect
```

23.3 green-ethernet short-reach (global)

Use the **green-ethernet short-reach** Global Configuration mode command to enable green-ethernet short-reach mode globally. Use the **no** form of this command to disabled it.

Syntax

green-ethernet short-reach

no green-ethernet short-reach

Parameters

N/A

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# green-ethernet short-reach
```

23.4 green-ethernet short-reach (interface)

Use the **green-ethernet short-reach** Interface Configuration mode command to enable green-ethernet short-reach mode on a port. Use the **no** form of this command to disable it on a port.

Syntax

green-ethernet short-reach

no green-ethernet short-reach

Parameters

N/A

Default Configuration

Disabled.

Command Mode
Interface Configuration mode (Ethernet)

User Guidelines
When **Short-Reach** mode is enabled and is not forced, the VCT (Virtual Cable Tester) length check must be performed. The VCT length check can be performed only on a copper port operating at a speed of 1000 Mbps. If the media is not copper or the link speed is not 1000 Mbps and short-reach mode is not forced (by green-ethernet short-reach force), Short-Reach mode is not applied.

When the interface is set to enhanced mode, after the VCT length check has completed and set the power to low, an active monitoring for errors is done continuously. In the case of errors crossing a certain threshold, the PHY will be reverted to long reach.

Note that EEE cannot be enabled if the Short-Reach mode is enabled.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# green-ethernet short-reach
```

23.5 green-ethernet short-reach force
Use the **green-ethernet short-reach force** Interface Configuration mode command to force short-reach mode on a port. Use the **no** form of this command to return to default.

Syntax
green-ethernet short-reach force

no green-ethernet short-reach force

Parameters
N/A

Default Configuration
Short-reach mode is not forced.

Command Mode
Interface Configuration mode (Ethernet)

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# green-ethernet short-reach force
```

23.6 green-ethernet short-reach threshold
Use the **green-ethernet short-reach threshold** Global Configuration mode command to set the maximum cable length for applying short-reach. Use the **no** form of this command to return to default.

Syntax

green-ethernet short-reach threshold *cable-length*

no green-ethernet short-reach threshold

Parameters

cable-length—Specifies the maximum cable length (in meters) measured by VCT that allows applying short-reach mode (cable-length 0–70 meters)

Default Configuration

The default length is 40 meters.

Command Mode

Global Configuration mode

User Guidelines

Note that the automatic cable length measurement accuracy is +-10 meters. i.e. a cable with a real length of 30 m may be evaluated in the range of 20m–40m. Length performance depends on the link partner signal quality, cable quality and whether the link partner also operates in short-reach mode.

Marvell recommends a default of 50m for any cable type.

However, Marvell tests show that the link partner can operate error free with a cable length of up to 80 m (cat 5e).

The user may choose to change the threshold parameter under certain circumstances.

Setting the threshold to 0 meters, basically results in the short reach feature always being disabled, because the threshold is always exceeded.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# green-ethernet short-reach threshold 30
```

23.7 green-ethernet power-meter reset

Use the **green-ethernet power meter reset** Privileged EXEC mode command to reset the power save meter.

Syntax

green-ethernet power-meter reset

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode.

Example

```
switchxxxxxx(config)# green-ethernet power-meter reset
```

23.8 show green-ethernet

Use the **show green-ethernet** Privileged EXEC mode command to display green-ethernet configuration and information.

Syntax

show green-ethernet *[interface-id]*

Parameters

interface-id—Specifies an Ethernet port.

Default Configuration

When no port is specified, information for all ports is displayed.

Command Mode

Privileged EXEC mode

User Guidelines

The following describes the reasons for non-operation displayed by this command.

If there are a several reasons, then only the highest priority reason is displayed.

Energy-detect Non-operational Reasons		
Priority	**Reason**	**Description**
1	NP	Port is not present
2	LT	Link Type is not supported (fiber, auto media select)
3	LU	Port Link is up – NA

Short-Reach Non-operational Reasons		
Priority	**Reason**	**Description**
1	NP	Port is not present
2	LT	Link Type is not supported (fiber)
3	LS	Link Speed Is not Supported (100M,10M,10G)
4	LL	Link Length received from VCT Test exceed threshold
6	LD	Port Link is Down – NA

Example

```
switchxxxxxx# show green-ethernet
Energy-Detect mode: Enabled
```

```
Short-Reach mode: Disabled
Power Consumption: 76% (3.31W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
Short-Reach cable length threshold: 50m
Port     Energy-Detect       Short-Reach           VCT Cable
      Admin Oper Reason   Admin Force Oper Reason   Length
----  ----- ---- -------  ----- ----- ---- -------  ------
fe1/0/11   on    on             off  off   off
fe1/0/12   on    off  LU        on   off   off           < 50
fe1/0/13   on    off  LU        off  off   off
```

24 Port Channel Commands

24.1 port-channel create

Use the **port-channel create** Global Configuration mode command to create a port channel. Use the **no** form of this command to remove the port-channel.

Syntax

port-channel create *port-channel*

no port-channel create *port-channel*

Parameters

port-channel—Specifies the port channel number. (Range: 1–64)

Default Configuration

No port channels exist.

Command Mode

Global Configuration mode

Example

The following example creates port-channel number 1.

```
switchxxxxxx(config)# port-channel create 1
```

24.2 channel-group

Use the **channel-group** Interface Configuration (Ethernet) mode command to associate a port with a port-channel. Use the **no** form of this command to remove a port from a port-channel.

Syntax

channel-group *port-channel* ***mode*** ***{on*** | ***auto}***

no channel-group

Parameters

- **port-channel**—Specifies the port channel number for the current port to join.
- **mode**—Specifies the mode of joining the port channel. The possible values are:
  - **on**—Forces the port to join a channel without an LACP operation.
  - **auto**—Forces the port to join a channel as a result of an LACP operation.

Default Configuration

The port is not assigned to a port-channel.

Command Mode
Interface Configuration (Ethernet) mode

Default mode is **on**.

Example
The following example forces port `fe1/0/11` to join port-channel 1 without an LACP operation.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# channel-group 1 mode on
```

24.3 port-channel load-balance
Use the **port-channel load-balance** Global Configuration mode command to configure the load balancing policy of the port channeling. Use the **no** form of this command to reset to default.

Syntax
port-channel load-balance ***{src-dst-mac*****| *src-dst-ip*** **|** ***src-dst-mac-ip}***

port-channel load-balance ***{src-dst-mac*****| *src-dst-ip*** **|** ***src-dst-mac-ip*** **|** ***src-dst-mac-ip-port}***

no port-channel load-balance

Parameters
- **src-dst-mac**—Port channel load balancing is based on the source and destination MAC address.
- **src-dst-mac-ip**—Port channel load balancing is based on the source and destination of MAC and IP addresses.
- **src-dst-mac-ip-port**—Port channel load balancing is based on the source and destination of MAC and IP addresses and on source and destination TCP/UDP port numbers.
- **src-dst-ip**—Port channel load balancing is based on the source and destination IP address.

Default Configuration
src-dst-mac is the default option.

Command Mode
Global Configuration mode

User Guidelines
In **src-dst-mac-ip-port** load balancing policy, fragmented packets might be reordered.

Example

```
switchxxxxxx(config)# port-channel load-balance src-dst-mac
switchxxxxxx(config)# port-channel load-balance src-dst-mac-ip
```

24.4 show interfaces port-channel

Use the **show interfaces port-channel** EXEC mode command to display port-channel information for all port channels or for a specific port channel.

Syntax

show interfaces port-channel *[interface-id]*

Parameters

interface-id—Specify an interface ID. The interface ID must be a Port Channel.

Command Mode

EXEC mode

Examples

Example 1 - The following example displays information on all port-channels.

```
switchxxxxxx# show interfaces port-channel
Load balancing: src-dst-mac.
Gathering information...
Channel  Ports
-------  -----
Po1      Active: fe1/0/11,Inactive: fe1/0/12-3
Po2      Active: fe1/0/15 Inactive: fe1/0/14
```

Example 2 - The following example displays information on port-channels containing port 1

```
switchxxxxxx# show interfaces switchport fe1/0/11
Gathering information...
Name: fe1/0/11
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs Enabled: 1
                        2-4094 (Inactive)
General PVID: 1
General VLANs Enabled: none
General Egress Tagged VLANs Enabled: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
```

```
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs Enabled: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN Enabled: none
DVA: disable
```

25 Address Table Commands

25.1 bridge multicast filtering

Use the **bridge multicast filtering** Global Configuration mode command to enable the filtering of Multicast addresses. Use the **no** form of this command to disable Multicast address filtering.

Syntax

bridge multicast filtering

no bridge multicast filtering

Default Configuration

Multicast address filtering is disabled. All Multicast addresses are flooded to all ports.

Command Mode

Global Configuration mode

User Guidelines

When this feature is enabled, unregistered Multicast traffic (as opposed to registered) will still be flooded.

All registered Multicast addresses will be forwarded to the Multicast groups. There are two ways to manage Multicast groups, one is the IGMP Snooping feature, and the other is the bridge multicast forward-all command.

Example

The following example enables bridge Multicast filtering.

```
switchxxxxxx(config)# bridge multicast filtering
```

25.2 bridge multicast mode

Use the **bridge multicast mode** Interface Configuration (VLAN) mode command to configure the Multicast bridging mode. Use the **no** form of this command to return to the default configuration.

Syntax

bridge multicast mode ***{mac-group*** | ***ip-group*** | ***ip-src-group}***

no bridge multicast mode

Parameters

- **mac-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address.
- **ipv4-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN and IPv4 destination address for IPv4 packets.

- **ipv4-src-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC address for non-IPv4 packets, and on the packet's VLAN, IPv4 destination address and IPv4 source address for IPv4 packets.

Default Configuration
The default mode is mac-group.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Use the mac-group option when using a network management system that uses a MIB based on the Multicast MAC address. Otherwise, it is recommended to use the ipv4-group or ipv4-src-group mode, because there is no overlapping of IPv4 Multicast addresses in these modes.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries in the FDB, as described in the following table:

FDB Mode	CLI Commands	
mac-group	bridge multicast address	bridge multicast forbidden address
ipv4-group	bridge multicast ip-address	bridge multicast forbidden ip-addresss
ipv4-src-group	bridge multicast source group	bridge multicast forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the IGMP version that is used in the network:

FDB mode	IGMP version 2	IGMP version 3
mac-group	MAC group address	MAC group address
ipv4-group	IP group address	IP group address
ipv4-src-group	(*)	IP source and group addresses

(*) Note that (*,G) cannot be written to the FDB if the mode is **ipv4-src-group**. In that case, no new FDB entry is created, but the port is added to the static (S,G) entries (if they exist) that belong to the requested group. It is recommended to set the FDB mode to ipv4-group or mac-group for IGMP version 2.

If an application on the device requests (*,G), the operating FDB mode is changed to ipv4-group.

Example
The following example configures the Multicast bridging mode as an ipv4-group on VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast mode ipv4-group
```

25.3 bridge multicast address

Use the **bridge multicast address** Interface Configuration (VLAN) mode command to register a MAC-layer Multicast address in the bridge table and statically add or remove ports to or from the group. Use the **no** form of this command to unregister the MAC address.

Syntax

bridge multicast address {*mac-multicast-address* | *ipv4-multicast-address*} ***[[add*** | ***remove]*** {***ethernet*** *interface-list* | **port-channel** *port-channel-list*}]

no bridge multicast address {*mac-multicast-address*}

Parameters

- **mac-multicast-address | ipv4-multicast-address**—Specifies the group Multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet interface-list**—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel port-channel-list**—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

If **ethernet interface-list** or **port-channel port-channel-list** is specified without specifying **add** or **remove**, the default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **mac-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Examples

Example 1 - The following example registers the MAC address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03
```

Example 2 - The following example registers the MAC address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 01:00:5e:02:02:03 add
fe1/0/11-2
```

25.4 bridge multicast forbidden address

Use the **bridge multicast forbidden address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific Multicast address to or from specific ports. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forbidden address {*mac-multicast-address* | *ipv4-multicast-address*} ***{add*** | ***remove}*** ***{ethernet*** *interface-list* | ***port-channel*** *port-channel-list*}

no bridge multicast forbidden address {*mac-multicast-address*}

Parameters

- **mac-multicast-address | ipv4-multicast-address**—Specifies the group Multicast address.
- **add**—Forbids adding ports to the group.
- **remove**—Forbids removing ports from the group.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered, using bridge multicast address.

You can execute the command before the VLAN is created.

Example

The following example forbids MAC address 0100.5e02.0203 on port `fe1/0/19` within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast address 0100.5e02.0203
switchxxxxxx(config-if)# bridge multicast forbidden address
0100.5e02.0203 add fe1/0/19
```

25.5 bridge multicast ip-address

Use the **bridge multicast ip-address** Interface Configuration (VLAN) mode command to register IP-layer Multicast addresses to the bridge table, and statically add or remove ports to or from the group. Use the no form of this command to unregister the IP address.

Syntax

bridge multicast ip-address *ip-multicast-address [[**add** | **remove**] {**ethernet** interface-list | **port-channel** port-channel-list}*]

no bridge multicast ip-address *ip-multicast-address*

Parameters

- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

Default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **ip-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Example

The following example registers the specified IP address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
```

The following example registers the IP address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2 add
fe1/0/19
```

25.6 bridge multicast forbidden ip-address

Use the **bridge multicast forbidden ip-address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP Multicast address to or from specific ports. Use the no form of this command to restore the default configuration.

Syntax

bridge multicast forbidden ip-address *{ip-multicast-address} {**add** | **remove**} {**ethernet** interface-list | **port-channel** port-channel-list}*

no bridge multicast forbidden ip-address {*ip-multicast-address*}

Parameters

- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Forbids adding ports to the group.
- **remove**—Forbids removing ports from the group.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers IP address 239.2.2.2, and forbids the IP address on port `fe1/0/19` within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ip-address 239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden ip-address
239.2.2.2 add fe1/0/19
```

25.7 bridge multicast source group

Use the **bridge multicast source group** Interface Configuration (VLAN) mode command to register a source IP address - Multicast IP address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the no form of this command to unregister the source-group-pair.

Syntax

bridge multicast source *ip-address* **group** *ip-multicast-address [[**add** | **remove**] {**ethernet** interface-list | **port-channel** port-channel-list}]*

no bridge multicast source *ip-address* **group** *ip-multicast-address*

Parameters

- **ip-address**—Specifies the source IP address.

- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Adds ports to the group for the specific source IP address.
- **remove**—Removes ports from the group for the specific source IP address.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

The default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

The following example registers a source IP address - Multicast IP address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group
239.2.2.2
```

25.8 bridge multicast forbidden source group

Use the **bridge multicast forbidden source group** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IP source address - Multicast address pair to or from specific ports. Use the no form of this command to return to the default configuration.

Syntax

bridge multicast forbidden source *ip-address* **group** *ip-multicast-address* {***add*** | ***remove***} {***ethernet*** *interface-list* | ***port-channel*** *port-channel-list*}

no bridge multicast forbidden source *ip-address* **group** *ip-multicast-address*

Parameters

- **ip-address**—Specifies the source IP address.
- **ip-multicast-address**—Specifies the group IP Multicast address.
- **add**—Forbids adding ports to the group for the specific source IP address.
- **remove**—Forbids removing ports from the group for the specific source IP address.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration
No forbidden addresses are defined.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example
The following example registers a source IP address - Multicast IP address pair to the bridge table, and forbids adding the pair to port `fe1/0/19` on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 13.16.1.1 group
239.2.2.2
switchxxxxxx(config-if)# bridge multicast forbidden source 13.16.1.1
group 239.2.2.2 add fe1/0/19
```

25.9 bridge multicast ipv6 mode
Use the **bridge multicast ipv6 mode** Interface Configuration (VLAN) mode command to configure the Multicast bridging mode for IPv6 Multicast packets. Use the no form of this command to return to the default configuration.

Syntax
bridge multicast ipv6 mode ***{mac-group*** | ***ip-group*** | ***ip-src-group}***

no bridge multicast ipv6 mode

Parameters
- **mac-group**—Specifies that Multicast bridging is based on the packet's VLAN and MAC destination address.
- **ip-group**—Specifies that Multicast bridging is based on the packet's VLAN and IPv6 destination address for IPv6 packets.
- **ip-src-group**—Specifies that Multicast bridging is based on the packet's VLAN, IPv6 destination address and IPv6 source address for IPv6 packets.

Default Configuration
The default mode is **mac-group**.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Use the **mac-group** mode when using a network management system that uses a MIB based on the Multicast MAC address.

For each Forwarding Data Base (FDB) mode, use different CLI commands to configure static entries for IPv6 Multicast addresses in the FDB, as described in the following table::

FDB Mode	CLI Commands	
mac-group	bridge multicast address	bridge multicast forbidden address
ipv6-group	bridge multicast ipv6 ip-address	bridge multicast ipv6 forbidden ip-address
ipv6-src-group	bridge multicast ipv6 source group	bridge multicast ipv6 forbidden source group

The following table describes the actual data that is written to the Forwarding Data Base (FDB) as a function of the MLD version that is used in the network:(*) Note that (*,G) cannot be written to the

FDB mode	MLD version 1	MLD version 2
mac-group	MAC group address	MAC group address
ipv6-group	IPv6 group address	IPv6 group address
ipv6-src-group	(*)	IPv6 source and group addresses

FDB if the mode is **ip-src-group**. In that case, no new FDB entry is created, but the port is added to the (S,G) entries (if they exist) that belong to the requested group. If an application on the device requests (*,G), the operating FDB mode is changed to **ip-group**.

You can execute the command before the VLAN is created.

Example

The following example configures the Multicast bridging mode as an **ip-group** on VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast ipv6 mode ip-group
```

25.10 bridge multicast ipv6 ip-address

Use the **bridge multicast ipv6 ip-address** Interface Configuration (VLAN) mode command to register an IPv6 Multicast address to the bridge table, and statically add or remove ports to or from the group. Use the **no** form of this command to unregister the IPv6 address.

Syntax

bridge multicast ipv6 ip-address *ipv6-multicast-address [[**add** | **remove**] {**ethernet** interface-list | **port-channel** port-channel-list}]*

no bridge multicast ipv6 ip-address *ip-multicast-address*

Parameters

- **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- **add**—Adds ports to the group.
- **remove**—Removes ports from the group.

- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No Multicast addresses are defined.

The default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

To register the group in the bridge database without adding or removing ports or port channels, specify the **ipv6-multicast-address** parameter only.

Static Multicast addresses can be defined on static VLANs only.

You can execute the command before the VLAN is created.

Example

Example 1 - The following example registers the IPv6 address to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address
FF00:0:0:0:4:4:4:1
```

Example 2 - The following example registers the IPv6 address and adds ports statically.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address
FF00:0:0:0:4:4:4:1 add fe1/0/11-2
```

25.11 bridge multicast ipv6 forbidden ip-address

Use the **bridge multicast ipv6 forbidden ip-address** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 Multicast address to or from specific ports. To restore the default configuration, use the **no** form of this command.

Syntax

bridge multicast ipv6 forbidden ip-address {*ipv6-multicast-address*} ***{add*** | ***remove}*** ***{ethernet*** *interface-list* | ***port-channel*** *port-channel-list}*

no bridge multicast ipv6 forbidden ip-address {*ipv6-multicast-address*}

Parameters

- **ipv6-multicast-address**—Specifies the group IPv6 Multicast address.
- **add**—Forbids adding ports to the group.

- **remove**—Forbids removing ports from the group.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

No forbidden addresses are defined.

The default option is **add**.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers an IPv6 Multicast address, and forbids the IPv6 address on port `fe1/0/19` within VLAN 8.

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast ipv6 ip-address
FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)# bridge multicast ipv6 forbidden ip-address
FF00:0:0:0:4:4:4:1 add fe1/0/19
```

25.12 bridge multicast ipv6 source group

Use the **bridge multicast ipv6 source group** Interface Configuration (VLAN) mode command to register a source IPv6 address - Multicast IPv6 address pair to the bridge table, and statically add or remove ports to or from the source-group. Use the **no** form of this command to unregister the source-group-pair.

Syntax

bridge multicast ipv6 source *ipv6-source-address* **group** *ipv6-multicast-address [[**add** | **remove**] {**ethernet** interface-list | **port-channel** port-channel-list}]*

no bridge multicast ipv6 source *ipv6-address* **group** *ipv6-multicast-address*

Parameters

- **ipv6-source-address**—Specifies the source IPv6 address.
- **ipv6-multicast-address**—Specifies the group IPv6 Multicast address.
- **add**—Adds ports to the group for the specific source IPv6 address.
- **remove**—Removes ports from the group for the specific source IPv6 address.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.

- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration
No Multicast addresses are defined.

The default option is **add**.

Command Mode
Interface Configuration (VLAN) mode

Example
The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group
FF00:0:0:0:4:4:4:1
```

25.13 bridge multicast ipv6 forbidden source group

Use the **bridge multicast ipv6 forbidden source group** Interface Configuration (VLAN) mode command to forbid adding or removing a specific IPv6 source address - Multicast address pair to or from specific ports. Use the **no** form of this command to return to the default configuration.

Syntax
bridge multicast ipv6 forbidden source *ipv6-source-address* **group** *ipv6-multicast-address {**add** | **remove**} {***ethernet*** *interface-list* | ***port-channel*** *port-channel-list}*

no bridge multicast ipv6 forbidden source *ipv6-address* **group** *ipv6-multicast-address*

Parameters
- **ipv6-source-address**—Specifies the source IPv6 address.
- **ipv6-multicast-address**—Specifies the group IPv6 multicast address.
- **add**—Forbids adding ports to the group for the specific source IPv6 address.
- **remove**—Forbids removing ports from the group for the specific source IPv6 address.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration
No forbidden addresses are defined.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines

Before defining forbidden ports, the Multicast group should be registered.

You can execute the command before the VLAN is created.

Example

The following example registers a source IPv6 address - Multicast IPv6 address pair to the bridge table, and forbids adding the pair to `fe1/0/19` on VLAN 8:

```
switchxxxxxx(config)# interface vlan 8
switchxxxxxx(config-if)# bridge multicast source 2001:0:0:0:4:4:4 group
FF00:0:0:0:4:4:4:1
switchxxxxxx(config-if)# bridge multicast forbidden source
2001:0:0:0:4:4:4:1 group FF00:0:0:0:4:4:4:1 add fe1/0/19
```

25.14 bridge multicast unregistered

Use the **bridge multicast unregistered** Interface Configuration (Ethernet, Port-Channel) mode command to configure forwarding unregistered Multicast addresses. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast unregistered ***{forwarding*** | ***filtering}***

no bridge multicast unregistered

Parameters

- **forwarding**—Forwards unregistered Multicast packets.
- **filtering**—Filters unregistered Multicast packets.

Default Configuration

Unregistered Multicast addresses are forwarded.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode

User Guidelines

Do not enable unregistered Multicast filtering on ports that are connected to routers, because the 224.0.0.x address range should not be filtered. Note that routers do not necessarily send IGMP reports for the 224.0.0.x range.

You can execute the command before the VLAN is created.

Example

The following example specifies that unregistered Multicast packets are filtered on `fe1/0/11`:

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# bridge multicast unregistered filtering
```

25.15 bridge multicast forward-all

Use the **bridge multicast forward-all** Interface Configuration (VLAN) mode command to enable forwarding all multicast packets for a range of ports or port channels. Use the **no** form of this command to restore the default configuration.

Syntax

bridge multicast forward-all ***{add*** | ***remove}*** ***{ethernet*** *interface-list* | ***port-channel*** *port-channel-list}*

no bridge multicast forward-all

Parameters

- **add**—Forces forwarding of all Multicast packets.
- **remove**—Does not force forwarding of all Multicast packets.
- **ethernet** *interface-list*—Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- **port-channel** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces. Use a hyphen to designate a range of port channels.

Default Configuration

Forwarding of all Multicast packets is disabled.

Command Mode

Interface Configuration (VLAN) mode

Example

The following example enables all Multicast packets on port fe1/0/18 to be forwarded.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forward-all add fe1/0/18
```

25.16 bridge multicast forbidden forward-all

Use the **bridge multicast forbidden forward-all** Interface Configuration (VLAN) mode command to forbid a port to dynamically join Multicast groups. Use the no form of this command to restore the default configuration.

Syntax

bridge multicast forbidden forward-all ***{add*** | ***remove}*** ***{ethernet*** *interface-list* | ***port-channel*** *port-channel-list}*

no bridge multicast forbidden forward-all

Parameters

- **add**—Forbids forwarding of all Multicast packets.
- **remove**—Does not forbid forwarding of all Multicast packets.

- ***ethernet*** *interface-list* —Specifies a list of Ethernet ports. Separate nonconsecutive Ethernet ports with a comma and no spaces. Use a hyphen to designate a range of ports.
- ***port-channel*** *port-channel-list*—Specifies a list of port channels. Separate nonconsecutive port-channels with a comma and no spaces; use a hyphen to designate a range of port channels.

Default Configuration
Ports are not forbidden to dynamically join Multicast groups.

The default option is **add**.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
Use this command to forbid a port to dynamically join (by IGMP, for example) a Multicast group.

The port can still be a Multicast router port.

Example
The following example forbids forwarding of all Multicast packets to fe1/0/11 within VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forbidden forward-all add
ethernet fe1/0/11
```

25.17 mac address-table static
Use the **mac address-table static** Global Configuration mode command to add a MAC-layer station source address to the MAC address table. Use the **no** form of this command to delete the MAC address.

Syntax
mac address-table static *mac-address* **vlan** *vlan-id* **interface** *interface-id* [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]

no mac address-table static [*mac-address]* ***vlan*** *vlan-id*

Parameters
- **mac-address**— MAC address (Range: Valid MAC address)
- **vlan-id**— Specify the VLAN
- **interface-id**— Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel (Range: valid ethernet port, valid port-channel)
- **permanent**— The permanent static MAC address. The keyword is applied by the default.
- **delete-on-reset**— The delete-on-reset static MAC address.
- **delete-on-timeout**— The delete-on-timeout static MAC address.
- **secure**—The secure MAC address. May be used only in a secure mode.

Default Configuration
No static addresses are defined. The default mode for an added address is permanent.

Command Mode
Global Configuration mode

User Guidelines
Use the command to add a static MAC address with given time-to-live in any mode or to add a secure MAC address in a secure mode.

Each MAC address in the MAC address table is assigned two attributes: **type** and **time-to-live**.

The following value of time-of-live is supported:

- **permanent**— a MAC address is saved until it is removed manually.
- **delete-on-reset**— a MAC address is saved until the next reboot.
- **delete-on-timeout**— a MAC address that may be removed by the aging timer.

The following types are supported:

- **static**— MAC address manually added by the command with the following keywords specifying its time-of-live:
  - **permanent**
  - **delete-on-reset**
  - **delete-on-timeout**

  A static MAC address may be added in any port mode.
- **secure**— A MAC address added manually or learned in a secure mode. Use the **mac address-table static** command with the **secure** keyword to add a secure MAC address address. The MAC address cannot be relearned.

  A secure MAC address may be added only in a secure port mode.
- **dynamic**— a MAC address learned by the switch in non secure mode. A value of its **time-to-live** attribute is **delete-on-timeout**.

Examples
Example 1 - The following example adds two permanent static MAC address:

```
switchxxxxxx(conf)#mac address-table static 00:3f:bd:45:5a:b1 vlan 1
fe1/0/11
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1
fe1/0/11 permanent
```

Example 2 - The following example adds a deleted-on-reset static MAC address:

```
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1
fe1/0/11 delete-on-reset
```

Example 3 - The following example adds a deleted-on-timeout static MAC address:

```
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1
fe1/0/11 delete-on-timeout
```

Example 4 - The following example adds a secure MAC address:

```
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1
fe1/0/11 secure
```

25.18 clear mac address-table

Use the **clear mac address-table** Privileged EXEC command to remove learned or secure entries from the forwarding database (FDB).

Syntax

clear mac address-table *dynamic [interface* *interface-id]*

clear mac address-table *secure interface* *interface-id*

Parameters

- **dynamic interface** *interface-id*—Delete all dynamic (learned) addresses on the specified interface.The interface ID can be one of the following types: Ethernet port or port-channel. If interface ID is not supplied, all dynamic addresses are deleted.
- **secure interface** *interface-id*—Delete all the secure addresses learned on the specific interface. A secure address on a MAC address learned on ports on which port security is defined.

Default Configuration

For dynamic addresses, if interface-id is not supplied, all dynamic entries are deleted.

Command Mode

Privileged EXEC mode

Examples:

Example 1 - Delete all dynamic entries from the FDB.

```
switchxxxxxx# clear mac address-table dynamic
```

Example 2 - Delete all secure entries from the FDB learned on secure port gi1.

```
switchxxxxxx# clear mac address-table secure interface gi1
```

25.19 mac address-table aging-time

Use the **mac address-table aging-time** Global configuration command to set the aging time of the address table. Use the **no** form of this command to restore the default.

Syntax

mac address-table aging-time *seconds*

no mac address-table aging-time

Parameters
seconds—Time is number of seconds. (Range:10–300)

Default Configuration
300

Command Mode
Global Configuration mode

Example

```
switchxxxxxx(config)# mac address-table aging-time 600
```

25.20 port security
Use the **port security** Interface Configuration (Ethernet, Port-channel) mode command to enable port security learning mode on an interface. Use the **no** form of this command to disable port security learning mode on an interface.

Syntax
port security [**forward** | **discard** | **discard-shutdown**] [**trap** *seconds*]

no port security

Parameters
- **forward**—Forwards packets with unlearned source addresses, but does not learn the address.
- **discard**—Discards packets with unlearned source addresses.
- **discard-shutdown**—Discards packets with unlearned source addresses and shuts down the port.
- **trap** *seconds*—Sends SNMP traps and specifies the minimum time interval in seconds between consecutive traps. (Range: 1–1000000)

Default Configuration
The feature is disabled by default.

The default mode is **discard**.

The default number of seconds is zero, but if **traps** is entered, a number of seconds must also be entered.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

See the mac address-table static command for information about MAC address attributes (type and time-to-live) definitions.

When the **port security** command enables the **lock** mode on a port all dynamic addresses learned on the port are changed to **permanent secure** addresses.

When the **port security** command enables a mode on a port differing from the **lock** mode all dynamic addresses learned on the port are deleted.

When the **no port security** command cancels a secure mode on a port all secure addresses defined on the port are changed to **dynamic** addresses.

Additionally to set a mode, use the **port security** command to set an action that the switch should perform on a frame which source MAC address cannot be learned.

Example

The following example forwards all packets to port fe1/0/11 without learning addresses of packets from unknown sources and sends traps every 100 seconds, if a packet with an unknown source address is received.

```
switchxxxxxx(config)interface fe1/0/17
switchxxxxxx(config-if)port security mode lock
switchxxxxxx(config-if)port security forward trap 100
switchxxxxxx(config-if)exit
```

25.21 port security mode

Use the **port security mode** Interface Configuration (Ethernet, port-channel) mode command configures the port security learning mode. Use the **no** form of this command to restore the default configuration.

Syntax

Parameters

- **max-addresses**— Non secure mode with limited learning dynamic MAC addresses. The static MAC addresses may be added on the port manually by the mac address-table static command.
- **lock**— Secure mode without MAC learning. The static and secure MAC addresses may be added on the port manually by the mac address-table static command.

Default Configuration

The default port security mode is **lock**.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The default port mode is called regular. In this mode, the port allows unlimited learning of dynamic addresses. The static MAC addresses may be added on the port manually by the mac address-table static command.

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use the **port security mode** command to change the default mode before the port security mode command.

Example
The following example sets the port security mode to Lock for fe1/0/17.

```
switchxxxxxx(config)interface fe1/0/17
switchxxxxxx(config-if)port security mode lock
switchxxxxxx(config-if)port security
switchxxxxxx(config-if)exit
```

25.22 port security max
Use the **port security max** Interface Configuration (Ethernet, Port-channel) mode command to configure the maximum number of addresses that can be learned on the port while the port is in port, max-addresses or secure mode. Use the **no** form of this command to restore the default configuration.

Syntax
port security max *max-addr*

no port security max

Parameters
max-addr—Specifies the maximum number of addresses that can be learned on the port. (Range: 0–256)

Default Configuration
This default maximum number of addresses is 1.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Use this command to change the default value before the port security command.

Example
The following example sets the port to limited learning mode:

```
switchxxxxxx(config)#interface gi7
switchxxxxxx(config-if)port security mode max
switchxxxxxx(config-if)port security max 20
switchxxxxxx(config-if)port security
switchxxxxxx(config-if)exit
```

25.23 port security routed secure-address

Use the **port security routed secure-address** Interface Configuration (Ethernet, Port-channel) mode command to add a MAC-layer secure address to a routed port. (port that has an IP address defined on it). Use the no form of this command to delete a MAC address from a routed port.

Syntax

port security routed secure-address *mac-address*

no port security routed secure-address [*mac-address*]

Parameters

mac-address—Specifies the MAC address.

Default Configuration

No addresses are defined.

Command Mode

Interface Configuration (Ethernet, port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command enables adding secure MAC addresses to a routed port in port security mode. The command is available when the port is a routed port and in port security mode. The address is deleted if the port exits the security mode or is not a routed port.

Example

The following example adds the MAC-layer address 00:66:66:66:66:66 to `fe1/0/1`1.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# port security routed secure-address
00:66:66:66:66:66
```

25.24 show mac address-table

Use the **show mac address-table** EXEC command to view entries in the MAC address table.

Syntax

show mac address-table ***[dynamic*** | ***static***| ***secure] [vlan*** *vlan] [**interface** interface-id] [**address** mac-address]*

Parameters

- **dynamic**—Displays only dynamic MAC address table entries.
- **static**—Displays only static MAC address table entries.
- **secure**—Displays only secure MAC address table entries.
- **vlan**—Displays entries for a specific VLAN.
- **interface-id**—SDisplays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

- **mac-address**—Displays entries for a specific MAC address.

Default Configuration
If no parameters are entered, the entire table is displayed.

Command Mode
EXEC mode

User Guidelines
Internal usage VLANs (VLANs that are automatically allocated on routed ports) are presented in the VLAN column by a port number and not by a VLAN ID.

Example
Example 1 - Displays entire address table.

```
switchxxxxxx# show mac address-table
Aging time is 300 sec
 VLAN        MAC Address         Port       Type
-------- ------------------- ---------- ----------
   1       00:00:26:08:13:23       0       self
   1       00:3f:bd:45:5a:b1     fe1/0/11       static
   1       00:a1:b0:69:63:f3     fe1/0/14       dynamic
   2       00:a1:b0:69:63:f3     fe1/0/15       dynamic
```

Example 2 - Displays address table entries containing the specified MAC address.

```
switchxxxxxx# show mac address-table 00:3f:bd:45:5a:b1
Aging time is 300 sec
VLAN        MAC Address         Port       Type
-------- ------------------- ---------- ----------
1         00:3f:bd:45:5a:b1    static      fe1/0/19
```

25.25 show mac address-table count

Use the **show mac address-table count** EXEC mode command to display the number of addresses present in the Forwarding Database.

Syntax
show mac address-table count ***[vlan*** *vlan* | ***interface*** *interface-id]*

Parameters
- **vlan**—Specifies VLAN.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode
EXEC mode

Example

```
switchxxxxxx# show mac address-table count
Capacity: 8192
Free: 8083
Used: 109
Secure   : 0
Dynamic  : 25
Static   : 1
Internal : 0
```

25.26 show bridge multicast mode

Use the **show bridge multicast mode** EXEC mode command to display the Multicast bridging mode for all VLANs or for a specific VLAN.

Syntax

show bridge multicast mode *[**vlan** vlan-id*]

Parameters

vlan *vlan-id*—Specifies the VLAN ID.

Command Mode

EXEC mode

Example

The following example displays the Multicast bridging mode for all VLANs.

```
switchxxxxxx# show bridge multicast mode
VLAN        IPv4 Multicast Mode        IPv6 Multicast Mode
      Admin          Oper           Admin          Oper
---   -----------    -----------    -----------    -----------
1     MAC-GROUP      MAC-GROUP      MAC-GROUP      -MAC-GROUP
11    IPv4-GROUP     IPv4-GROUP     IPv6-GROUP     IPv6-GROUP
12    IPv4-SRC-      IPv4-SRC-      IPv6-SRC-      IPv6-SRC-
      GROUP          GROUP          GROUP          GROUP
```

25.27 show bridge multicast address-table

Use the **show bridge multicast address-table** EXEC mode command to display Multicast MAC addresses or IP Multicast address table information.

Syntax

show bridge multicast address-table *[**vlan** vlan-id] [**address** {mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address}] [**format** {**ip** | **mac**}] [**source** {ipv4-source-address | ipv6-source-address}*]

Parameters

- **vlan-id***vlan-id*—Display entries for specified VLAN ID.
- **address** —Display entries for specified Multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC Multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 Multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 Multicast address.
- **format**—(this applies if picked mac-multicast-address). then i can display it either in mac or ip format) Display entries for specified Multicast address format. The possible values are:
  - **ip**—Specifies that the Multicast address is an IP address.
  - **mac**—Specifies that the Multicast address is a MAC address.
- **source {ipv4-source-address | ipv6-source-address}**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

Default Configuration

If the **format** is not specified, it defaults to **mac** (only if mac-multicast-address was entered).

If VLAN ID is not entered, entries for all VLANs are displayed.

If MAC or IP address is not supplied, entries for all addresses are displayed.

Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000 through 0100.5e7f.ffff.

Multicast router ports (defined statically or discovered dynamically) are members in all MAC groups.

Ports that were defined via the bridge multicast forbidden forward-all command are displayed in all forbidden MAC entries.

Changing the Multicast mode can move static Multicast addresses that are written in the device FDB to a shadow configuration because of FDB hash collisions.

Example

The following example displays bridge Multicast address information.

```
switchxxxxxx# show bridge multicast address-table
Multicast address table for VLANs in MAC-GROUP bridging mode:
Vlan    MAC Address         Type           Ports
---- -----------------    --------------   -----
8    01:00:5e:02:02:03     Static          1-2


Forbidden ports for Multicast addresses:
Vlan    MAC Address         Ports
---- -----------------      -----
8    01:00:5e:02:02:03      fe1/0/19
```

```
Multicast address table for VLANs in IPv4-GROUP bridging mode:
Vlan    MAC Address         Type             Ports
---- -----------------    --------------     -----
1      224.0.0.251         Dynamic           fe1/0/12
Forbidden ports for Multicast addresses:
Vlan    MAC Address         Ports
---- -----------------      -----
1      232.5.6.5
1      233.22.2.6
Multicast address table for VLANs in IPv4-SRC-GROUP bridging mode:
Vlan  Group Address  Source address  Type        Ports
---- --------------- --------------- --------    -----
1     224.2.2.251     11.2.2.3       Dynamic     fe1/0/11
Forbidden ports for Multicast addresses:
Vlan  Group Address  Source Address   Ports
---- --------------- --------------- -------
8    239.2.2.2       *               fe1/0/19
8    239.2.2.2       1.1.1.11        fe1/0/19
Multicast address table for VLANs in IPv6-GROUP bridging mode:
VLAN  IP/MAC Address   Type      Ports
---- ----------------- --------- --------------------
8    ff02::4:4:4       Static    fe1/0/11-2, fe1/0/17, Po1
Forbidden ports for Multicast addresses:
VLAN  IP/MAC Address   Ports
---- ----------------- -----------
8    ff02::4:4:4       fe1/0/19
Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:
Vlan  Group Address  Source address  Type     Ports
---- --------------- --------------- -------- ------------------
8    ff02::4:4:4     *               Static   fe1/0/11-2,fe1/0/17,Po1
8    ff02::4:4:4     fe80::200:7ff:  Static
                     fe00:200
Forbidden ports for Multicast addresses:
Vlan  Group Address  Source address  Ports
---- --------------- --------------- ----------
8    ff02::4:4:4     *               fe1/0/19
8    ff02::4:4:4     fe80::200:7ff:f    fe1/0/19
                     e00:200
```

25.28 show bridge multicast address-table static

Use the **show bridge multicast address-table static** EXEC mode command to display the statically configured Multicast addresses.

Syntax

show bridge multicast address-table static *[**vlan** vlan-id] [**address** mac-multicast-address | ipv4-multicast-address | ipv6-multicast-address] [**source** ipv4-source-address | ipv6-source-address] [**all** | **mac** | **ip**]*

Parameters

- **vlan vlan-id**—Specifies the VLAN ID.
- **address**—Specifies the Multicast address. The possible values are:
  - **mac-multicast-address**—Specifies the MAC Multicast address.
  - **ipv4-multicast-address**—Specifies the IPv4 Multicast address.
  - **ipv6-multicast-address**—Specifies the IPv6 Multicast address.
- **source**—Specifies the source address. The possible values are:
  - **ipv4-address**—Specifies the source IPv4 address.
  - **ipv6-address**—Specifies the source IPv6 address.

Default Configuration

When **all/mac/ip** is not specified, all entries (MAC and IP) will be displayed.

Command Mode

EXEC mode

User Guidelines

A MAC address can be displayed in IP format only if it is within the range 0100.5e00.0000–-0100.5e7f.ffff.

Example

The following example displays the statically configured Multicast addresses.

```
switchxxxxxx# show bridge multicast address-table static
MAC-GROUP table

Vlan       MAC Address        Ports
----       --------------     --------
1          0100.9923.8787     fe1/0/11, fe1/0/12

Forbidden ports for multicast addresses:

Vlan       MAC Address        Ports
----       --------------     --------

IPv4-GROUP Table

Vlan       IP Address         Ports
----       ----------         --------
1          231.2.2.3          fe1/0/11, fe1/0/12
19         231.2.2.8          fe1/0/1-8
19         231.2.2.8          fe1/0/19-21

Forbidden ports for multicast addresses:
```

```
Vlan       IP Address         Ports
----       ----------         --------
1          231.2.2.3          fe1/0/18
19         231.2.2.8          fe1/0/13

IPv4-SRC-GROUP Table:

Vlan       Group Address      Source               Ports
----       ---------------    address              ------
                              ---------------

Forbidden ports for multicast addresses:

Vlan       Group Address      Source               Ports
----       ---------------    address              ------
                              ---------------

IPv6-GROUP Table

Vlan       IP Address         Ports
----       ----------------   ---------
191        -                  fe1/0/11-8
           FF12::8

Forbidden ports for multicast addresses:

Vlan       IP Address         Ports
----       ----------------   ---------
11         -                  fe1/0/18
191        FF12::3            fe1/0/18
           FF12::8

IPv6-SRC-GROUP Table:

Vlan       Group Address      Source               Ports
----       ---------------    address              ------
192        FF12::8            ---------------      fe1/0/11-8
                              FE80::201:C9A9:FE40
                              :8988

Forbidden ports for multicast addresses:

Vlan       Group Address      Source               Ports
----       ---------------    address              ------
192        FF12::3            ---------------      fe1/0/18
                              FE80::201:C9A9:FE40
                              :8988
```

25.29 show bridge multicast filtering

Use the **show bridge multicast filtering** EXEC mode command to display the Multicast filtering configuration.

Syntax

show bridge multicast filtering *vlan-id*

Parameters
vlan-id—Specifies the VLAN ID. (Range: Valid VLAN)

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example displays the Multicast configuration for VLAN 1.

```
switchxxxxxx# show bridge multicast filtering 1
Filtering: Enabled
VLAN: 1

Port         Forward-All
-----        Static         Status
fe1/0/11     ---------      ------
fe1/0/12     Forbidden      Filter
fe1/0/13     Forward        Forward(s)
             -              Forward(d)
```

25.30 show bridge multicast unregistered
Use the **show bridge multicast unregistered** EXEC mode command to display the unregistered Multicast filtering configuration.

Syntax
show bridge multicast unregistered *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
Display for all interfaces.

Command Mode
EXEC mode

Example
The following example displays the unregistered Multicast configuration.

```
switchxxxxxx# show bridge multicast unregistered

Port        Unregistered
-------     -------------
fe1/0/11    Forward
fe1/0/12    Filter
fe1/0/13    Filter
```

25.31 show ports security
Use the **show ports security** Privileged EXEC mode command to display the port-lock status.

Syntax
show ports security *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
Display for all interfaces.

Command Mode
Privileged EXEC mode

Example
The following example displays the port-lock status of all ports.

```
switchxxxxxx# show ports security

Port    Status     Learning    Action    Maximum  Trap     Frequency
------- --------  ---------   ------    ---      -------  --------
fe1/0/11     Enabled   Max-        Discard   3         Enabled 100
                  Addresses
fe1/0/12     Disabled  Max-        -         28        -        -
                  Addresses
fe1/0/13     Enabled   Lock        Discard, 8          Disabled -
                                   Shutdown
```

The following table describes the fields shown above.

Field	Description
Port	The port number.
Status	The port security status. The possible values are: Enabled or Disabled.
Action	The action taken on violation.
Maximum	The maximum number of addresses that can be associated on this port in the Max-Addresses mode.
Trap	The status of SNMP traps. The possible values are: Enable or Disable.
Frequency	The minimum time interval between consecutive traps.

25.32 show ports security addresses

Use the **show ports security addresses** Privileged EXEC mode command to display the current dynamic addresses in locked ports.

Syntax

show ports security addresses [*interface-id*

Parameters

interface-id—Display addresses for the specified interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Display for all interfaces.

Command Mode

Privileged EXEC mode

Example

The following example displays dynamic addresses in all currently locked port:

```
Port    Status      Learning        Current    Maximum
-------  --------    ---------------  ----------  ----------
gi1     Disabled    Lock            0          10
gi2     Disabled    Lock            0          1
gi3     Disabled    Lock            0          1
gi4     Disabled    Lock            0          1
gi5     Disabled    Lock            0          1
gi6     Disabled    Lock            0          1
gi7     Disabled    Lock            0          1
...
```

25.33 bridge multicast reserved-address

Use the **bridge multicast reserved-address** Global Configuration mode command to define the action on Multicast reserved-address packets. Use the **no** form of this command to revert to default.

Syntax

bridge multicast reserved-address *mac-multicast-address* ***[ethernet-v2*** *ethtype* | ***llc*** *sap* | ***llc-snap*** *pid]* ***{discard*** | ***bridge}***

no bridge multicast reserved-address *mac-multicast-address* ***[ethernet-v2*** *ethtype* | ***llc*** *sap* | ***llc-snap*** *pid]*

Parameters

- **mac-multicast-address**—MAC Multicast address in the reserved MAC addresses range.(Range: 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-2F)
- **ethernet-v2** *ethtype*—Specifies that the packet type is Ethernet v2 and the Ethernet type field (16 bits in hexadecimal format).(Range: 0x0600–0xFFFF)
- **llc** *sap*—Specifies that the packet type is LLC and the DSAP-SSAP field (16 bits in hexadecimal format).(Range: 0xFFFF)
- **llc-snap** *pid*—Specifies that the packet type is LLC-SNAP and the PID field (40 bits in hexadecimal format). (Range: 0x0000000000 - 0xFFFFFFFFFF)
- **discard**—Specifies discarding the packets.
- **bridge**—Specifies bridging (forwarding) the packets

Default Configuration

- If the user-supplied MAC Multicast address, ethertype and encapsulation (LLC) specifies a protocol supported on the device (called Peer), the default action (discard or bridge) is determined by the protocol.
- If not, the default action is as follows:
  - For MAC addresses in the range 01-80-C2-00-00-00, 01-80-C2-00-00-02–01-80-C2-00-00-0F, the default is **discard**.
  - For MAC addresses in the range 00-80-C2-00-00-10– 01-80-C2-00-00-2F, the default is **bridge**.

Command Mode

Global Configuration mode

User Guidelines

If the packet/service type (ethertype/encapsulation) is not specified, the configuration is relevant to all the packets with the configured MAC address.

Specific configurations (that contain service type) have precedence over less specific configurations (contain only MAC address).

The packets that are bridged are subject to security ACLs.

The actions define by this command has precedence over forwarding rules defined by applications/protocols (STP, LLDP etc.) supported on the device.

Example

```
switchxxxxxx(conf)#bridge multicast reserved-address 00:3f:bd:45:5a:b1
```

25.34 show bridge multicast reserved-addresses

Use the **show bridge multicast reserved-addresses** EXEC mode command to display the Multicast reserved-address rules.

Syntax

show bridge multicast reserved-addresses

Command Mode

EXEC mode

Example

```
switchxxxxxx # show bridge multicast reserved-addresses
MAC Address         Frame Type  Protocol        Action
------------------  ----------- --------------  ------------
01-80-C2-00-00-00   LLC-SNAP    00-00-0C-01-29  Bridge
```

26 Port Monitor Commands

26.1 port monitor

Use the **port monitor** Interface Configuration (Ethernet) mode command to start a port monitoring session (mirroring). Use the **no** form of this command to stop a port monitoring session.

Syntax

port monitor *src-interface-id [**rx** | **tx**]*

no port monitor *src-interface-id*

port monitor ***vlan*** *vlan-id*

no port monitor ***vlan*** *vlan-id*

Parameters

- **rx**—Monitors received packets only. If no option is specified, it monitors both rx and tx.
- **tx**—Monitors transmitted packets only. If no option is specified, it monitors both rx and tx.
- **vlan** *vlan-id*—VLAN number
- **src-interface-id**—Specifies an interface ID. The interface ID must be and Ethernet port.

Default Configuration

Monitors both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command enables port copy between Source Port (src-interface) to a Destination Port (The port in context).

The analyzer port for port ingress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for port egress traffic mirroring should be the same port for all mirrored ports.

The analyzer port for VLAN mirroring should be the same for all the mirrored VLANs, and should be the same port as the analyzer port for port ingress mirroring traffic.

The following restriction applies to ports that are configured to be source ports:

- The port cannot be a destination port.

The following restrictions apply to ports that are configured to be monitor ports:

- The port cannot be source port.
- The port is not a member in port-channel.
- IP interface is not configured on the port.
- GVRP is not enabled on the port.
- The port is not a member in any VLAN, except for the default VLAN (will be automatically removed from the default VLAN).
- L2 protocols, such as: LLDP, CDP, LBD, STP, LACP, are not active on the destination port.

Notes:

1. In this mode some traffic duplication on the analyzer port may be observed. For example:
   - Port 2 is being egress monitored by port 4.
   - Port 2 & 4 are members in VLAN 3.
   - Unknown Unicast packet sent to VLAN 3 will egress from port 4 twice, one instance as normal forward and another instance as mirrored from port 2.
   - Moreover, if port 2 is an untagged member in VLAN 3 and port 4 is a tagged member then both instances will look different (one tagged and the other is not).
2. When the port is configured to 802.1X auto mode it will forward any mirrored traffic regardless of the.1X state. However, it will operate as a normal network port (forward traffic) only after authorization is done.
3. Mirrored traffic is exposed to STP state, i.e. if the port is in STP blocking, it will not egress any mirrored traffic.

Example

The following example copies traffic for both directions (Tx and Rx) from the source port `fe1/0/12` to destination port `fe1/0/11`.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# port monitor fe1/0/12
```

26.2 show ports monitor

Use the **show ports monitor** EXEC mode command to display the port monitoring status.

Syntax

show ports monitor

Command Mode

EXEC mode

Example

The following example displays the port monitoring status.

```
switchxxxxxx# show ports monitor
Source port     Destination Port   Type      Status
-----------   ----------------    --------  --------
fe1/0/18            fe1/0/11               RX,TX     Active
fe1/0/12            fe1/0/11               RX,TX     Active
fe1/0/118        fe1/0/11            Rx        Active
VLAN 9          fe1/0/11            N/A       Active
```

26.3 port monitor mode

Use the **port monitor mode** Global Configuration mode command to define the monitoring mode. Use the **no** form of this command to return to default.

Syntax

port monitor mode ***{monitor-only*** | ***network}***

no port monitor mode

Parameters

- **monitor-only**—Specifies that the monitor port acts only as a monitor port. Other network traffic is discarded at ingress and egress.
- **network**—Specifies that the monitor port acts also as a network port.

Default Configuration

The default is monitor-only.

Command Mode

Global Configuration mode

User Guidelines

Once the port monitor mode is defined, no changing between modes is allowed. Any mode change will have to first go through un-defining the monitor port.

Example

```
switchxxxxxx(config)# port monitor mode network
```

27 sFlow Commands

27.1 sflow receiver

Use the **sflow receiver** Global Configuration mode command to define sFlow collector. Use the **no** form of this command to remove the definition of the collector.

Syntax

sflow receiver *index {ipv4-address | ipv6-address | hostname} [port port] [max-datagram-size bytes]*

no sflow receiver *index*

Parameters

- **index**—The index of the receiver. (Range: 1–8)
- **ipv4-address**—Pv4 address of the host to be used as an sFlow Collector.
- **ipv6-address**—IPv6 address of the host to be used as an sFlow Collector. When the IPv6 address is a Link Local address (IPv6Z address), the outgoing interface name must be specified. Refer to the User Guidelines for the interface name syntax.
- **hostname**—Hostname of the host to be used as an sFlow Collector. Only translation to IPv4 addresses is supported.
- **port**—Port number for sflow messages. If unspecified, the port number defaults to 6343. The range is 1-65535.
- **bytes**—Specifies the maximum datagramsize that can be sent. If unspecified, it defaults to 1400.

Default

No receiver is defined.

Command Mode

Global Configuration mode

User Guidelines

If the IP address of the sFlow receiver is set to 0.0.0.0, no sFlow datagrams are sent.

27.2 sflow flow-sampling

Use the **sflow flow-sampling** Interface Configuration mode command to enable sFlow Flow sampling and configure the average sampling rate of a specific port. Use the **no** form of this command to disable Flow sampling.

Syntax

sflow flow-sampling *rate receiver-index [max-header-size bytes]*

no sflow flow-sampling

Parameters

- **rate**—Specifies the average sampling rate (Range: 1, 1024–1073741823.)
- **receiver-index**—Index of the receiver/collector (Range: 1–8.)
- **bytes**—Specifies the maximum number of bytes that would be copied from the sampled packet. If unspecified, defaults to 128. (Range: 20–256.)

Default

Disabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

A new sampling rate configuration is not immediately loaded to the hardware. It will be loaded to the hardware only after the next packet is sampled (based on the current sampling rate).

27.3 sflow counters-sampling

Use the **sflow counters-sampling** Interface Configuration mode command to enable sFlow Counters sampling and to configure the maximum interval of a specific port. Use the **no** form of this command to disable sFlow Counters sampling.

Syntax

sflow counters-sampling *interval receiver-index*

no sflow counters-sampling

Parameters

- **interval**—Specifies the maximum number of seconds between successive samples of the interface counters. (Range: 1, 15–86400.)
- **receiver-index**—Index of the receiver/collector. (Range: 1–8.)

Default

Disabled

Command Mode

Interface Configuration (Ethernet) mode

27.4 clear sflow statistics

Use the **clear sFlow statistics** EXEC mode command to clear sFlow statistics.

Syntax

clear sflow statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode
EXEC mode

User Guidelines
If no interface is specified by the user, the command clears all the sFlow statistics counters (including datagrams sent). If an interface is specified by the user, the command clears only the counter of the specific interface.

27.5 show sflow configuration
Use the **show sflow configuration** EXEC mode command to display the sFlow configuration for ports that are enabled for Flow sampling or Counters sampling.

Syntax
show sflow configuration *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode
EXEC mode

Example
```
Console # show sflow configuration
Receivers
Index      IP Address        Port   Max Datagram Size
----- ------------------- -------- ----------------
  1         0.0.0.0          6343         1400
  2         172.16.1.2       6343         1400
  3         0.0.0.0          6343         1400
  4         0.0.0.0          6343         1400
  5         0.0.0.0          6343         1400
  6         0.0.0.0          6343         1400
  7         0.0.0.0          6343         1400
  8         0.0.0.0          6343         1400
Interfaces
Inter-  Flow          Counters  Max Header  Flow      Counters Collector
face    Sampling      Sampling  Size        Collector Index    Index
----- -----------     --------- ---------   ---------- -----   ------------
fe1/0/11   1/2048     60 sec    128         1                  1
fe1/0/12   1/4096     Disabled  128         0                  2
```

27.6 show sflow statistics

Use the **show sflow statistics** EXEC mode command to display the sFlow statistics for ports that are enabled for Flow sampling or Counters sampling.

Syntax

show sflow statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

EXEC mode

Example

```
Console # show sflow statistics
Total sFlow datagrams sent to collectors: 100
```

Interface	Packets sampled	Datagrams sent to collector
fe1/0/11	30	50
fe1/0/12	30	50
fe1/0/13	30	50

28 Link Layer Discovery Protocol (LLDP) Commands

28.1 lldp run

Use the **lldp run** Global Configuration mode command to enable LLDP. To disable LLDP, use the **no** form of this command.

Syntax

lldp run

no lldp run

Parameters

N/A.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

```
console(config)# lldp run
```

28.2 lldp transmit

Use the **lldp transmit** Interface Configuration mode command to enable transmitting LLDP on an interface. Use the **no** form of this command to stop transmitting LLDP on an interface.

Syntax

lldp transmit

no lldp transmit

Parameters

N/A

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

LLDP manages LAG ports individually. LLDP sends separate advertisements on each port in a LAG.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are sent on blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
console(config)# interface fe1/0/11
console(config-if)# lldp transmit
```

28.3 lldp receive

Use the **lldp receive** Interface Configuration mode command to enable receiving LLDP on an interface. Use the **no** form of this command to stop receiving LLDP on an interface.

Syntax

lldp receive

no lldp receive

Parameters

N/A

Default Configuration

Enabled

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

LLDP manages LAG ports individually. LLDP data received through LAG ports is stored individually per port.

LLDP operation on a port is not dependent on the STP state of a port. I.e. LLDP frames are received on blocked ports.

If a port is controlled by 802.1x, LLDP operates only if the port is authorized.

Example

```
console(config)# interface fe1/0/11
console(config-if)# lldp receive
```

28.4 lldp timer

Use the **lldp timer** Global Configuration mode command to specify how often the software sends LLDP updates. Use the **no** form of this command to restore the default configuration.

Syntax
lldp timer *seconds*

no lldp timer

Parameters
timer *seconds*—Specifies, in seconds, how often the software sends LLDP updates (range: 5-32768 seconds).

Default Configuration
30 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the interval for sending LLDP updates to 60 seconds.

```
Console(config)# lldp timer 60
```

28.5 lldp hold-multiplier
Use the **lldp hold-multiplier** Global Configuration mode command to specify how long the receiving device holds a LLDP packet before discarding it. Use the **no** form of this command to restore the default configuration.

Syntax
lldp hold-multiplier *number*

no lldp hold-multiplier

Parameters
hold-multiplier *number*—Specifies the LLDP packet hold time interval as a multiple of the LLDP timer value (range: 2-10).

Default Configuration
The default LLDP hold multiplier is 4.

Command Mode
Global Configuration mode

User Guidelines
The actual Time-To-Live (TTL) value of LLDP frames is calculated by the following formula:

TTL = min(65535, LLDP-Timer * LLDP-hold-multiplier)

For example, if the value of the LLDP timer is 30 seconds, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field of the LLDP header.

Example
The following example sets the LLDP packet hold time interval to 90 seconds.

```
Console(config)# lldp timer 30
Console(config)# lldp hold-multiplier 3
```

28.6 lldp reinit
Use the **lldp reinit** Global Configuration mode command to specify the minimum time an LLDP port waits before reinitializing LLDP transmission. Use the **no** form of this command to revert to the default setting.

Syntax
lldp reinit *seconds*

no lldp reinit

Parameters
reinit *seconds*—Specifies the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission.(Range: 1–10)

Default Configuration
2 seconds

Command Mode
Global Configuration mode

Example

```
console(config)# lldp reinit 4
```

28.7 lldp tx-delay
Use the **lldp tx-delay** Global Configuration mode command to set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Use the **no** form of this command to restore the default configuration.

Syntax
lldp tx-delay *seconds*

no lldp tx-delay

Parameters
tx-delay *seconds*—Specifies the delay in seconds between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB (range: 1-8192 seconds).

Default Configuration
The default LLDP frame transmission delay is 2 seconds.

Command Mode
Global Configuration mode

User Guidelines
It is recommended that the tx-delay be less than 0.25 of the LLDP timer interval.

Example
The following example sets the LLDP transmission delay to 10 seconds.

```
Console(config)# lldp tx-delay 10
```

28.8 lldp management-address
Use the **lldp management-address** Interface Configuration (Ethernet) mode command to specify the management address advertised by an interface. Use the **no** form of this command to stop advertising management address information.

Syntax
lldp management-address *{ip-address* | ***none*** | ***automatic*** *[interface-id]}*

no lldp management-address

Parameters
- **ip-address**—Specifies the static management address to advertise.
- **none**—Specifies that no address is advertised.
- **automatic**—Specifies that the software automatically selects a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses.
- **automatic** *interface-id*—(Available only when the device is in Layer 3 (router mode)). Specifies that the software automatically selects a management address to advertise from the IP addresses that are configured on the interface ID. In case of multiple IP addresses, the software selects the lowest IP address among the dynamic IP addresses of the interface. If there are no dynamic addresses, the software selects the lowest IP address among the static IP addresses of the interface. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN. Note that if the port or port- channel are members in a VLAN that has an IP address, that address is not included because the address is associated with the VLAN.

Default Configuration
No IP address is advertised.

The default advertisement is **automatic**.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
Each port can advertise one IP address.

Example

The following example sets the LLDP management address advertisement mode to **automatic** on `fe1/0/12`.

```
Console(config)# interface fe1/0/12
Console(config-if)# lldp management-address automatic
```

28.9 lldp notifications

Use the **lldp notifications** Interface Configuration (Ethernet) mode command to enable/disable sending LLDP notifications on an interface. Use the **no** form of this command to restore the default configuration.

Syntax

lldp notifications *{**enable** | **disable**}*

no lldp notifications

Parameters

- **enable**—Enables sending LLDP notifications.
- **disable**—Disables sending LLDP notifications.

Default Configuration

Disabled.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables sending LLDP notifications on `fe1/0/15`.

```
Console(config)# interface fe1/0/15
Console(config-if)# lldp notifications enable
```

28.10 lldp notifications interval

Use the **lldp notifications interval** Global Configuration mode command to configure the maximum transmission rate of LLDP notifications. Use the **no** form of this command to return to the default.

Syntax

lldp notifications interval *seconds*

no lldp notifications interval

Parameters

interval *seconds*—The device does not send more than a single notification in the indicated period (range: 5–3600).

Default Configuration
5 seconds

Command Mode
Global Configuration mode

Example

```
console(config)# lldp notifications interval 10
```

28.11 lldp optional-tlv 802.1

Use the **lldp optional-tlv** Interface Configuration mode command to specify which optional TLVs to transmit. Use the **no** form of this command to revert to the default setting.

Syntax
lldp optional-tlv 802.1 pvid - The PVID is advertised.

no lldp optional-tlv 802.1 pvid - The PVID is not advertised

lldp optional-tlv 802.1 ppvid *add* *ppvid* - The Protocol Port VLAN ID (PPVID) is advertised. The PPVID is the PVID that is used depending on the packet's protocol.

lldp optional-tlv 802.1 ppvid *remove* *ppvid* - The PPVID is not advertised.

lldp optional-tlv 802.1 vlan *add* *vlan-id* - This *vlan-id* is advertised.

lldp optional-tlv 802.1 vlan *remove* *vlan-id* - This *vlan-id* is not advertised.

lldp optional-tlv 802.1 protocol *add* *{**stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp**}* - The protocols selected are advertised.

lldp optional-tlv 802.1 protocol *remove* *{**stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp**}* - The protocols selected are not advertised.

Parameters
- **lldp optional-tlv 802.1 pvid**—Advertises the PVID of the port.
- **lldp optional-tlv 802.1 ppvid add/remove** *ppvid*—Adds/removes PPVID for advertising. (range: 0–4094). PPVID = 0 indicates that the port is not capable of supporting port and protocol VLANs and/or the port is not enabled with any protocol VLANs.
- **add/remove** *vlan-id*—Adds/removes VLAN for advertising (range: 0–4094).
- **add/remove** *{**stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp**}*—Add specifies to advertise the specified protocols; remove specifies not to advertise the specified protocol.

Default Configuration
No optional TLV is transmitted.

Command Mode
Interface Configuration (Ethernet) mode

Example

```
console(config)# lldp  optional-tlv 802.1 protocol add stp
```

28.12 lldp lldpdu

The **lldp lldpdu** Global Configuration mode command defines LLDP packet handling when LLDP is globally disabled. To restore the default configuration, use the **no** form of this command.

Syntax

lldp lldpdu {***filtering*** | ***flooding***}

no lldp lldpdu

Parameters

- **filtering** — Specifies that when LLDP is globally disabled, LLDP packets are filtered (deleted).
- **flooding** — Specifies that when LLDP is globally disabled, LLDP packets are flooded (forwarded to all interfaces).

Default Configuration

LLDP packets are filtered when LLDP is globally disabled.

Command Mode

Global Configuration mode

User Guidelines

If the STP mode is MSTP, the LLDP packet handling mode cannot be set to **flooding**.

The STP mode cannot be set to MSTP if the LLDP packet handling mode is **flooding**.

If LLDP is globally disabled, and the LLDP packet handling mode is **flooding**, LLDP packets are treated as data packets with the following exceptions:

- VLAN ingress rules are not applied to LLDP packets. The LLDP packets are trapped on all ports for which the STP state is Forwarding.
- Default "deny-all" rules are not applied to LLDP packets.
- VLAN egress rules are not applied to LLDP packets. The LLDP packets are flooded to all ports for which the STP state is Forwarding.
- LLDP packets are sent as untagged.

Example

The following example sets the LLDP packet handling mode to Flooding when LLDP is globally disabled.

```
Console(config)# lldp lldpdu flooding
```

28.13 lldp med enable

Use the **lldp med enable** Interface Configuration (Ethernet) mode command to enable LLDP Media Endpoint Discovery (MED) on an interface. Use the **no** form of this command to disable LLDP MED on an interface.

Syntax

lldp med enable [*tlv* … *tlv4*]

no lldp med enable

Parameters
tlv—Specifies the TLVs that should be included. Available TLVs are: network-policy, location, poe-pse, and inventory. The capabilities TLV is always included if LLDP-MED is enabled.

Default Configuration
LLDP MED is enabled.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example enables LLDP MED with the **location** TLV on `fe1/0/1`3.

```
Console(config)# interface fe1/0/13
Console(config-if)# lldp med enable location
```

28.14 lldp med notifications topology-change
Use the **lldp med notifications topology-change** Interface Configuration (Ethernet) mode command to enable sending LLDP MED topology change notifications on a port. Use the **no** form of this command to restore the default configuration.

Syntax
lldp med notifications topology-change ***{enable*** | ***disable}***

no lldp med notifications topology-change

Parameters
- **enable**—Enables sending LLDP MED topology change notifications.
- **disable**—Disables sending LLDP MED topology change notifications.

Default Configuration
Disable is the default.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example enables sending LLDP MED topology change notifications on `fe1/0/1`2.

```
Console(config)# interface fe1/0/12
Console(config-if)# lldp med notifications topology-change enable
```

28.15 lldp med fast-start repeat-count

When a port comes up, LLDP can send packets more quickly than usual using its fast-start mechanism.

Use the **lldp med fast-start repeat-count** Global Configuration mode command to configure the number of packets that is sent during the activation of the fast start mechanism. Use the **no** form of this command return to default.

Syntax

lldp med fast-start repeat-count *number*

no lldp med fast-start repeat-count

Parameters

repeat-count *number*—Specifies the number of times the fast start LLDPDU is being sent during the activation of the fast start mechanism. The range is 1-10.

Default Configuration

3

Command Mode

Global Configuration mode

Example

```
console(config)# lldp med fast-start repeat-count 4
```

28.16 lldp med network-policy (global)

Use the **lldp med network-policy** Global Configuration mode command to define a LLDP MED network policy. For voice applications, it is simpler to use lldp med network-policy voice auto.

The **lldp med network-policy** command creates the network policy, which is attached to a port by lldp med network-policy (interface).

The network policy defines how LLDP packets are constructed.

Use the **no** form of this command to remove LLDP MED network policy.

Syntax

lldp med network-policy *number application [**vlan** vlan-id] [**vlan-type** {**tagged** | **untagged**}] [**up** priority] [**dscp** value]*

no lldp med network-policy *number*

Parameters

- **number**—Network policy sequential number. The range is 1-32.
- **application**—The name or the number of the primary function of the application defined for this network policy. Available application names are:
  - voice
  - voice-signaling

- guest-voice
- guest-voice-signaling
- softphone-voice
- video-conferencing
- streaming-video
- video-signaling.

- **vlan** *vlan-id*—VLAN identifier for the application.
- **vlan-type**—Specifies if the application is using a tagged or an untagged VLAN.
- **up** *priority*—User Priority (Layer 2 priority) to be used for the specified application.
- **dscp** *value*—DSCP value to be used for the specified application.

Default Configuration
No network policy is defined.

Command Mode
Global Configuration mode

User Guidelines
Use the **lldp med network-policy** Interface Configuration command to attach a network policy to a port.

Up to 32 network policies can be defined.

Example
This example creates a network policy for the voice-signally application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
console(config)# lldp med network-policy 1 voice-signaling vlan 1
vlan-type untagged up 1 dscp 2
Console(config)# interface fe1/0/11
Console(config-if)# lldp med network-policy add 1
```

28.17 lldp med network-policy (interface)
Use the **lldp med network-policy** Interface Configuration (Ethernet) mode command to attach or remove an LLDP MED network policy on a port. Network policies are created in lldp med network-policy (global).

Use the **no** form of this command to remove all the LLDP MED network policies from the port.

Syntax
lldp med network-policy ***{add*** | ***remove}*** *number*

no lldp med network-policy *number*

Parameters
- **number**—Specifies the network policy sequential number. The range is 1-32
- **add/remove** *number*—Attaches/removes the specified network policy to the interface.

Default Configuration
No network policy is attached to the interface.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
For each port, only one network policy per application (voice, voice-signaling, etc.) can be defined.

Example
This example creates a network policy for the voice-signally application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
console(config)# lldp med network-policy 1 voice-signaling vlan 1
vlan-type untagged up 1 dscp 2
Console(config)# interface fe1/0/11
Console(config-if)# lldp med network-policy add 1
```

28.18 clear lldp table
Use the **clear lldp table** command in Privileged EXEC mode to clear the neighbors table for all ports or for a specific port.

Syntax
clear lldp table *[interface-id]*

Parameters
interface-id—Specifies a port ID.

Default Configuration
If no interface is specified, the default is to clear the LLDP table for all ports.

Command Mode
Privileged EXEC mode

Example

```
console# clear lldp table fe1/0/11
```

28.19 lldp med location
Use the **lldp med location** Interface Configuration (Ethernet) mode command to configure the location information for the LLDP Media Endpoint Discovery (MED) for a port. Use the **no** form of this command to delete location information for a port.

Syntax
lldp med location *{{**coordinate** data} | {**civic-address** data} | {**ecs-elin** data}}*

no lldp med location *{**coordinate** | **civic-address** | **ecs-elin**}*

Parameters

- **coordinate** *data*—Specifies the location data as coordinates in hexadecimal format.
- **civic-address** *data*—Specifies the location data as a civic address in hexadecimal format.
- **ecs-elin** *data*—Specifies the location data as an Emergency Call Service Emergency Location Identification Number (ECS ELIN) in hexadecimal format.
- **data**—Specifies the location data in the format defined in ANSI/TIA 1057: dotted hexadecimal data: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. (Length: coordinate: 16 bytes. Civic-address: 6-160 bytes. Ecs-elin: 10-25 bytes)

Default Configuration

The location is not configured.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example configures the LLDP MED location information on `fe1/0/12` as a civic address.

```
console(config)# interface fe1/0/12
console(config-if)# lldp med location civic-address 616263646566
```

28.20 show lldp configuration

Use the **show lldp configuration** Privileged EXEC mode command to display the LLDP configuration for all ports or for a specific port.

Syntax

show lldp configuration *[interface-id]*

Parameters

interface-id—Specifies the port ID.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

Example 1 - Display LLDP configuration for all ports.

```
Switch# show lldp configuration
State: Enabled
```

```
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Port      State  Optional TLVs      Address       Notifications
--------  -----  --------------      -------       ------------
fe1/0/11       RX,TX  PD, SN, SD, SC      172.16.1.1    Disabled
fe1/0/12       TX     PD, SN             172.16.1.1    Disabled
fe1/0/13       RX,TX  PD, SN, SD, SC      None          Disabled
fe1/0/15       RX,TX  D,  SN, SD, SC      automatic     Disabled
fe1/0/16       RX,TX  PD, SN, SD, SC      auto vlan 1   Disabled
fe1/0/17       RX,TX  PD, SN, SD, SC      auto g1       Disabled
fe1/0/18   RX,TX  PD, SN, SD, SC      auto ch1      Disabled
```

Example 2 - Display LLDP configuration for port 1.

```
Switch# show lldp configuration fe1/0/11
 State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Port State    Optional TLVs     Address      Notifications
------------- -------------- ------------------------
fe1/0/11  RX, TX   PD, SN, SD, SC    72.16.1.1    Disabled
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x
```

The following table describes the significant fields shown in the display:

Field	Description
Timer	The time interval between LLDP updates.
Hold multiplier	The amount of time (as a multiple of the timer interval) that the receiving device holds a LLDP packet before discarding it.
Reinit timer	The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.
Tx delay	The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.

Field	Description
Port	The port number.
State	The port's LLDP state.
Optional TLVs	Optional TLVs that are advertised. Possible values are: PD - Port description SN - System name SD - System description SC - System capabilities
Address	The management address that is advertised.
Notifications	Indicates whether LLDP notifications are enabled or disabled.
PVID	Port VLAN ID advertised.
PPVID	Protocol Port VLAN ID advertised.
Protocols	Protocols advertised.

28.21 show lldp med configuration

Use the **show lldp med configuration** Privileged EXEC mode command to display the LLDP Media Endpoint Discovery (MED) configuration for all ports or for a specific port.

Syntax

show lldp med configuration *[interface-id]*

Parameters

interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following example displays the LLDP MED configuration for all interfaces.

```
console# show lldp med configuration
Fast Start Repeat Count: 4.
Network policy 1
-------------------
Application type: voiceSignaling
VLAN ID: 1  untagged
Layer 2 priority: 0
DSCP: 0
Port    Capabilities   Network Policy Location  Notifications  Inventory
------ -------------- -------------- ---------- -------------   --------
fe1/0/11    Yes             Yes            Yes         Enabled        Yes
```

```
fe1/0/12    Yes             Yes             No          Enabled        No
fe1/0/13    No              No              No          Enabled        No
```

Example 2 - The following example displays the LLDP MED configuration for fe1/0/11.

```
console# show lldp med configuration fe1/0/11

Port    Capabilities   Network Policy   Location  Notifications Inventory
------- -------------- ---------------- --------- ----------    --------
fe1/0/11     Yes             Yes             Yes       Enabled        Yes
Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

28.22 show lldp local tlvs-overloading

When an LLDP packet contains too much information for one packet, this is called overloading. Use the **show lldp local tlvs-overloading** EXEC mode command to display the status of TLVs overloading of the LLDP on all ports or on a specific port.

Syntax

show lldp local tlvs-overloading *[interface-id]*

Parameters

interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

EXEC mode

User Guidelines

The command calculates the overloading status of the current LLDP configuration, and not for the last LLDP packet that was sent.

Example

```
Switch# show lldp local tlvs-overloading fe1/0/11
TLVs Group             Bytes       Status
------------           ------      --------------
Mandatory               31         Transmitted
LLDP-MED Capabilities   9          Transmitted
LLDP-MED Location       200        Transmitted
802.1                   1360       Overloading
Total: 1600 bytes
```

```
Left: 100 bytes
```

28.23 show lldp local

Use the **show lldp local** Privileged EXEC mode command to display the LLDP information that is advertised from a specific port.

Syntax

show lldp local *interface-id*

Parameters

Interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode

Example

The following examples display LLDP information that is advertised from `fe1/0/1`1 and 2.

```
Switch# show lldp local fe1/0/11
Device ID: 0060.704C.73FF
Port ID: fe1/0/11
Capabilities: Bridge
System Name: ts-7800-1
System description:
Port description:
Management address: 172.16.1.8
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
1000BASE-T full duplex
Operational MAU type: 1000BaseTFD
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
802.3 Maximum Frame Size: 1522
802.3 EEE
Local Tx: 30 usec
Local Rx: 25 usec
Remote Tx Echo: 30 usec
Remote Rx Echo: 25 usec
```

```
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2 (VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy, Location Identification
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice
Flags: Tagged VLAN
VLAN ID: 2
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power source: Primary Power Source
Power priority: High
Power value: 9.6 Watts
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
Hardware Revision: B1
Firmware Revision: A1
Software Revision: 3.8
Serial number: 7978399
Manufacturer name: Manufacturer
Model name: Model 1
Asset ID: Asset 123
Switch# show lldp local fe1/0/12
LLDP is disabled.
```

28.24 show lldp neighbors

Use the **show lldp neighbors** Privileged EXEC mode command to display information about neighboring devices discovered using LLDP. The information can be displayed for all ports or for a specific port.

Syntax

show lldp neighbors *[interface-id]*

Parameters

interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

Privileged EXEC mode

User Guidelines

A TLV value that cannot be displayed as an ASCII string is displayed as an hexadecimal string.

Examples

Example 1 - The following example displays information about neighboring devices discovered using LLDP on all ports on which LLDP is enabled and who are up.

Location information, if it exists, is also displayed.

```
Switch# show lldp neighbors
Port  Device ID         Port ID  System Name Capabilities TTL
----- ---------------   -------- ----------  -----------  ----
fe1/0/11 00:00:00:11:11:11    fe1/0/11     ts-7800-2    B            90
fe1/0/11 00:00:00:11:11:11 D  fe1/0/11     ts-7800-2    B            90
fe1/0/12 00:00:26:08:13:24    fe1/0/13     ts-7900-1    B, R         90
fe1/0/13 00:00:26:08:13:24    fe1/0/12     ts-7900-2    W            90
```

Example 2 - The following example displays information about neighboring devices discovered using LLDP on port 1.

```
Switch# show lldp neighbors fe1/0/11
Device ID: 00:00:00:11:11:11
Port ID: fe1/0/11
System Name: ts-7800-2
Capabilities: B
System description:
Port description:
Management address: 172.16.1.1
Time To Live: 90 seconds
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported.
Auto-negotiation status: Enabled.
Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
1000BASE-T full duplex.
Operational MAU type: 1000BaseTFD
802.3 Power via MDI
MDI Power support Port Class: PD
PSE MDI Power Support: Not Supported
PSE MDI Power State: Not Enabled
PSE power pair control ability: Not supported.
PSE Power Pair: Signal
PSE Power class: 1
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 1
```

```
802.3 Maximum Frame Size: 1522
802.3 EEE
Remote Tx: 25 usec
Remote Rx: 30 usec
Local Tx Echo: 30 usec
Local Rx Echo: 25 usec
802.1 PVID: 1
802.1 PPVID: 2 supported, enabled
802.1 VLAN: 2(VLAN2)
802.1 Protocol: 88 8E 01
LLDP-MED capabilities: Network Policy.
LLDP-MED Device type: Endpoint class 2.
LLDP-MED Network policy
Application type: Voice
Flags: Unknown policy
VLAN ID: 0
Layer 2 priority: 0
DSCP: 0
LLDP-MED Power over Ethernet
Device Type: Power Device
Power source: Primary power
Power priority: High
Power value: 9.6 Watts
Hardware revision: 2.1
Firmware revision: 2.3
Software revision: 2.7.1
Serial number: LM759846587
Manufacturer name: VP
Model name: TR12
Asset ID: 9
LLDP-MED Location
Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

The following table describes significant LLDP fields shown in the display:

Field	Description
Port	The port number.
Device ID	The neighbor device's configured ID (name) or MAC address.
Port ID	The neighbor device's port ID.
System name	The neighbor device's administratively assigned name.

Field	Description
Capabilities	The capabilities discovered on the neighbor device. Possible values are: B - Bridge R - Router W - WLAN Access Point T - Telephone D - DOCSIS cable device H - Host r - Repeater O - Other
System description	The neighbor device's system description.
Port description	The neighbor device's port description.
Management address	The neighbor device's management address.
Auto-negotiation support	The auto-negotiation support status on the port. (supported or not supported)
Auto-negotiation status	The active status of auto-negotiation on the port. (enabled or disabled)
Auto-negotiation Advertised Capabilities	The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.
Operational MAU type	The port MAU type.
LLDP MED	
Capabilities	The sender's LLDP-MED capabilities.
Device type	The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.
LLDP MED - Network Policy	
Application type	The primary function of the application defined for this network policy.
Flags	Flags. The possible values are: Unknown policy: Policy is required by the device, but is currently unknown. Tagged VLAN: The specified application type is using a tagged VLAN. Untagged VLAN: The specified application type is using an Untagged VLAN.
VLAN ID	The VLAN identifier for the application.
Layer 2 priority	The Layer 2 priority used for the specified application.
DSCP	The DSCP value used for the specified application.
LLDP MED - Power Over Ethernet	
Power type	The device power type. The possible values are: Power Sourcing Entity (PSE) or Power Device (PD).

Field	Description
Power Source	The power source utilized by a PSE or PD device. A PSE device advertises its power capability. The possible values are: Primary power source and Backup power source. A PD device advertises its power source. The possible values are: Primary power, Local power, Primary and Local power.
Power priority	The PD device priority. A PSE device advertises the power priority configured for the port. A PD device advertises the power priority configured for the device. The possible values are: Critical, High and Low.
Power value	The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
LLDP MED - Location	
Coordinates, Civic address, ECS ELIN.	The location information raw data.

28.25 show lldp statistics

Use the show **lldp statistics** EXEC mode command to display LLDP statistics on all ports or a specific port.

Syntax

show lldp statistics *[interface-id]*

Parameters

interface-id—Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

EXEC mode

Example

```
Switch# show lldp statistics
console(config-if)# do show lldp statistics
Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1
     TX Frames     RX Frame                RX  TLVs            RX Ageouts
```

Port	Total	Total Discarded	Errors	Discarded	Unrecognized	Total
fe1/0/11	730	850	0	0	0	0	0
fe1/0/12	0	0	0	0	0	0	0
fe1/0/13	730	0	0	0	0	0	0
fe1/0/14	0	0	0	0	0	0	0
fe1/0/15	0	0	0	0	0	0	0
fe1/0/16	8	7	0	0	0	0	1
fe1/0/17	0	0	0	0	0	0	0
fe1/0/18	0	0	0	0	0	0	0
fe1/0/19	730	0	0	0	0	0	0
fe1/0/110	0	0	0	0	0	0	0

29 Spanning-Tree Commands

29.1 spanning-tree

Use the **spanning-tree** Global Configuration mode command to enable spanning-tree functionality. Use the **no** form of this command to disable the spanning-tree functionality.

Syntax

spanning-tree

no spanning-tree

Parameters

N/A

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

Example

The following example enables spanning-tree functionality.

```
switchxxxxxx(config)# spanning-tree
```

29.2 spanning-tree mode

Use the **spanning-tree mode** Global Configuration mode command to select which Spanning Tree Protocol (STP) protocol to run. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mode ***{stp*** | ***rstp*** | ***mst}***

no spanning-tree mode

Parameters

- **stp**—Specifies that STP is enabled.
- **rstp**—Specifies that the Rapid STP is enabled.
- **mst**—Specifies that the Multiple STP is enabled.

Default Configuration

The default is RSTP.

Command Mode

Global Configuration mode

User Guidelines

In RSTP mode, the device uses STP when the neighbor device uses STP.

In MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

Example

The following example enables MSTP.

```
switchxxxxxx(config)# spanning-tree mode mstp
```

29.3 spanning-tree forward-time

Use the **spanning-tree forward-time** Global Configuration mode command to configure the spanning-tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Parameters

seconds—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration

15 seconds.

Command Mode

Global Configuration mode

User Guidelines

When configuring the forwarding time, the following relationship should be maintained:

2*(Forward-Time - 1) >= Max-Age

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds.

```
switchxxxxxx(config)# spanning-tree forward-time 25
```

29.4 spanning-tree hello-time

Use the **spanning-tree hello-time** Global Configuration mode command to configure how often the device broadcasts Hello messages to other devices. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree hello-time *seconds*

no spanning-tree hello-time

Parameters
seconds—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration
2 seconds.

Command Mode
Global Configuration mode

User Guidelines
When configuring the Hello time, the following relationship should be maintained:

Max-Age >= 2*(Hello-Time + 1)

Example
The following example configures the spanning-tree bridge hello time to 5 seconds.

```
switchxxxxxx(config)# spanning-tree hello-time 5
```

29.5 spanning-tree max-age
Use the **spanning-tree max-age** Global Configuration mode command to configure the STP maximum age. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree max-age *seconds*

no spanning-tree max-age

Parameters
seconds—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration
The default maximum age is 20 seconds.

Command Mode
Global Configuration mode

User Guidelines
When configuring the maximum age, the following relationships should be maintained:

2*(Forward-Time - 1) >= Max-Age

Max-Age >= 2*(Hello-Time + 1)

Example
The following example configures the spanning-tree bridge maximum age to 10 seconds.

```
switchxxxxxx(config)# spanning-tree max-age 10
```

29.6 spanning-tree priority
Use the **spanning-tree priority** Global Configuration mode command to configure the device STP priority, which is used to determine which bridge is selected as the root bridge. Use the **no** form of this command to restore the default device spanning-tree priority.

Syntax
spanning-tree priority *priority*

no spanning-tree priority

Parameters
priority—Specifies the bridge priority. (Range: 0–61440)

Default Configuration
Default priority = 32768.

Command Mode
Global Configuration mode

User Guidelines
The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree. When more than one switch has the lowest priority, the switch with the lowest MAC address is selected as the root.

Example
The following example configures the spanning-tree priority to 12288.

```
switchxxxxxx(config)# spanning-tree priority 12288
```

29.7 spanning-tree disable
Use the **spanning-tree disable** Interface Configuration (Ethernet, port-channel) mode command to disable the spanning tree on a specific port. Use the **no** form of this command to enable the spanning tree on a port.

Syntax
spanning-tree disable

no spanning-tree disable

Parameters
N/A

Default Configuration
Spanning tree is enabled on all ports.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example disables the spanning tree on `fe1/0/15`

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# spanning-tree disable
```

29.8 spanning-tree cost
Use the **spanning-tree cost** Interface Configuration (Ethernet, port-channel) mode command to configure the spanning-tree path cost for a port. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree cost *cost*

no spanning-tree cost

Parameters
cost—Specifies the port path cost. (Range: 1–200000000)

Default Configuration
Default path cost is determined by port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example configures the spanning-tree cost on `fe1/0/1`15 to 35000.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# spanning-tree cost 35000
```

29.9 spanning-tree port-priority

Use the **spanning-tree port-priority** Interface Configuration (Ethernet, port-channel) mode command to configure the port priority. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree port-priority *priority*

no spanning-tree port-priority

Parameters

priority—Specifies the port priority. (Range: 0–240)

Default Configuration

The default port priority is 128.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on `fe1/0/1`15 to 96

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# spanning-tree port-priority 96
```

29.10 spanning-tree portfast

Use the **spanning-tree portfast** Interface Configuration (Ethernet, port-channel) mode command to enable the PortFast mode. In PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay. Use the **no** form of this command to disable the PortFast mode.

Syntax

spanning-tree portfast [**auto**]

no spanning-tree portfast

Parameters

auto—Specifies that the software waits for 3 seconds (with no Bridge Protocol Data Units (BPDUs) received on the interface) before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is disabled.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example enables the PortFast mode on `fe1/0/1`15.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# spanning-tree portfast
```

29.11 spanning-tree link-type
Use the **spanning-tree link-type** Interface Configuration (Ethernet, port-channel) mode command to override the default link-type setting determined by the port duplex mode, and enable RSTP transitions to the Forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree link-type ***{point-to-point*** | ***shared}***

no spanning-tree spanning-tree link-type

Parameters
- **point-to-point**—Specifies that the port link type is point-to-point.
- **shared**—Specifies that the port link type is shared.

Default Configuration
The device derives the port link type from the duplex mode. A full-duplex port is considered a point-to-point link and a half-duplex port is considered a shared link.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example enables shared spanning-tree on `fe1/0/11`5.

```
switchxxxxxx(config)# interface fe1/0/115
switchxxxxxx(config-if)# spanning-tree link-type shared
```

29.12 spanning-tree pathcost method
Use the **spanning-tree pathcost method** Global Configuration mode command to set the default path cost method. Use the **no** form of this command to return to the default configuration.

Syntax
spanning-tree pathcost method ***{long*** | ***short}***

no spanning-tree pathcost method

Parameters

- **long**—Specifies that the default port path costs are within the range: 1–200,000,000.
- **short**—Specifies that the default port path costs are within the range: 1–65,535.

Default Configuration

Long path cost method.

Command Mode

Global Configuration mode

User Guidelines

This command applies to all the spanning tree instances on the switch.

- If the short method is selected, the switch calculates cost in the range 1 through 65,535.
- If the long method is selected, the switch calculates cost in the range 1 through 200,000,000.

Example

The following example sets the default path cost method to Long.

```
switchxxxxxx(config)# spanning-tree pathcost method long
```

29.13 spanning-tree bpdu (Global)

Use the **spanning-tree bpdu** Global Configuration mode command to define Bridge Protocol Data Unit (BPDU) handling when the spanning tree is disabled globally or on a single interface. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree bpdu *{**filtering** | **flooding**}*

no spanning-tree bpdu

Parameters

- **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to all ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The default setting is **flooding**.

Command Mode

Global Configuration mode

User Guidelines

The **filtering** and **flooding** modes are relevant when the spanning tree is disabled globally or on a single interface.

Example

The following example defines the BPDU packet handling mode as **flooding** when the spanning tree is disabled on an interface.

```
switchxxxxxx(config)# spanning-tree bpdu flooding
```

29.14 spanning-tree bpdu (Interface)

Use the **spanning-tree bpdu** Interface Configuration (Ethernet, Port-channel) mode command to define BPDU handling when the spanning tree is disabled on a single interface. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree bpdu ***{filtering*** | ***flooding}***

no spanning-tree bpdu

Parameters

- **filtering**—Specifies that BPDU packets are filtered when the spanning tree is disabled on an interface.
- **flooding**—Specifies that untagged BPDU packets are flooded unconditionally (without applying VLAN rules) to ports with the spanning tree disabled and BPDU handling mode of flooding. Tagged BPDU packets are filtered.

Default Configuration

The spanning-tree bpdu (Global) command determines the default configuration.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example defines the BPDU packet as **flooding** when the spanning tree is disabled on `fe1/0/13`.

```
switchxxxxxx(config)# interface fe1/0/13
switchxxxxxx(config-if)# spanning-tree bpdu flooding
```

29.15 spanning-tree guard root

use the **spanning-tree guard root** Interface Configuration (Ethernet, Port-channel) mode command to enable Root Guard on all spanning-tree instances on the interface. Root guard prevents the interface from becoming the root port of the device. Use the **no** form of this command to disable the root guard on the interface.

Syntax

spanning-tree guard root

no spanning-tree guard root

Default Configuration
Root guard is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
Root Guard can be enabled when the device operates in any mode (STP, RSTP and MSTP).

When Root Guard is enabled, the port changes to the alternate state if the spanning-tree calculations select the port as the root port.

Example
The following example prevents `fe1/0/11` from being the root port of the device.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# spanning-tree guard root
```

29.16 spanning-tree bpduguard
Use the **spanning-tree bpduguard** Interface Configuration (Ethernet, port-channel) mode command to shut down an interface when it receives a Bridge Protocol Data Unit (BPDU). Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree bpduguard ***{enable*** | ***disable}***

no spanning-tree bpduguard

Parameters
bpduguard *enable*—Enables BPDU Guard.

bpduguard *disable*—Disables BPDU Guard.

Default Configuration
BPDU Guard is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
The command can be enabled when the spanning tree is enabled (useful when the port is in the PortFast mode) or disabled.

Example
The following example shuts down `fe1/0/15` when it receives a BPDU.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# spanning-tree bpduguard enable
```

29.17 clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** Privileged EXEC command to restart the STP migration process (force renegotiation with neighboring switches) on all interfaces or on the specified interface

Syntax

clear spanning-tree detected-protocols ***[interface*** *interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All interfaces.

Command Mode

Privileged EXEC mode

User Guidelines

This feature can only be used when working in RSTP or MSTP mode.

Example

This restarts the STP migration process on all interfaces.

```
switchxxxxxx# clear spanning-tree detected-protocols
```

29.18 spanning-tree mst priority

Use the **spanning-tree mst priority** Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst *instance-id* ***priority*** *priority*

no spanning-tree mst *instance-id* ***priority***

Parameters

- **instance-id**—Specifies the spanning-tree instance ID. (Range:1–7)
- **priority**—Specifies the device priority for the specified spanning-tree instance. This setting determines the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0–61440)

Default Configuration

The default priority is 32768.

Command Mode
Global Configuration mode

User Guidelines
The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example
The following example configures the spanning tree priority of instance 1 to 4096.

```
switchxxxxxx(config)# spanning-tree mst 1 priority 4096
```

29.19 spanning-tree mst max-hops
Use the **spanning-tree mst max-hops** Global Configuration mode command to configure the number of hops in an MST region before the BDPU is discarded and the port information is aged out. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Parameters
max-hops *hop-count*—Specifies the number of hops in an MST region before the BDPU is discarded. (Range: 1–40)

Default Configuration
The default number of hops is 20.

Command Mode
Global Configuration mode

Example
The following example configures the maximum number of hops that a packet travels in an MST region before it is discarded to 10.

```
switchxxxxxx(config)# spanning-tree mst max-hops 10
```

29.20 spanning-tree mst port-priority
Use the **spanning-tree mst port-priority** Interface Configuration (Ethernet, port-channel) mode command to configure the priority of a port. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Parameters
- **instance-id**—Specifies the spanning tree instance ID. (Range: 1–15)
- **priority**—Specifies the port priority. (Range: 0–240 in multiples of 16)

Default Configuration
The default port priority is 128.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The priority value must be a multiple of 16.

Example
The following example configures the port priority of fe1/0/11 to 144.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# spanning-tree mst 1 port-priority 144
```

29.21 spanning-tree mst cost

Use the **spanning-tree mst cost** Interface Configuration (Ethernet, Port-channel) mode command to configure the path cost for MST calculations. If a loop occurs, the spanning tree considers path cost when selecting an interface to put in the Forwarding state. Use the **no** form of this command to restore the default configuration.

Syntax
spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Default Configuration
N/A

Parameters
- **instance-id**—Specifies the spanning-tree instance ID. (Range: 1–15)
- **cost**—Specifies the port path cost. (Range: 1–200000000)

Default Configuration
Default path cost is determined by the port speed and path cost method (long or short) as shown below:

Interface	Long	Short
Port-channel	20,000	4
TenGigabit Ethernet (10000 Mbps)	2000	2

Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
The following example configures the MSTP instance 1 path cost for gigabitethernet port 9 to 4.

```
switchxxxxxx(config)# interface fe1/0/19
switchxxxxxx(config-if)# spanning-tree mst 1 cost 4
```

29.22 spanning-tree mst configuration
Use the **spanning-tree mst configuration** Global Configuration mode command to enable configuring an MST region by entering the MST mode.

Syntax
spanning-tree mst configuration

Command Mode
Global Configuration mode

User Guidelines
For two or more switches to be in the same MST region, they must contain the same VLAN mapping, the same configuration revision number, and the same name.

Example
The following example configures an MST region.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
switchxxxxxx(config-mst)# name region1
switchxxxxxx(config-mst)# revision 1
```

29.23 instance (MST)
Use **instance** MST Configuration mode command to map VLANs to an MST instance. Use the **no** form of this command to restore the default mapping.

Syntax
instance *instance-id* ***vlan*** *vlan-range*

no **instance** *instance-id* ***vlan*** *vlan-range*

Parameters

- **instance-id**—MST instance (Range: 1–15)
- **vlan-range**—The specified range of VLANs is added to the existing ones. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 1–4094)

Default Configuration

All VLANs are mapped to the common and internal spanning tree (CIST) instance (instance 0).

Command Mode

MST Configuration mode

User Guidelines

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST.

For two or more devices to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

Example

The following example maps VLANs 10-20 to MST instance 1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1 vlan 10-20
```

29.24 name (MST)

Use the **name** MST Configuration mode command to define the MST instance name. Use the **no** form of this command to restore the default setting.

Syntax

name *string*

no name

Parameters

string—Specifies the MST instance name. (Length: 1–32 characters)

Default Configuration

The default name is the bridge MAC address.

Command Mode

MST Configuration mode

Example

The following example defines the instance name as Region1.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

29.25 revision (MST)

Use the **revision** MST Configuration mode command to define the MST configuration revision number. Use the **no** form of this command to restore the default configuration.

Syntax

revision *value*

no revision

Parameters

value—Specifies the MST configuration revision number. (Range: 0–65535)

Default Configuration

The default configuration revision number is 0.

Command Mode

MST Configuration mode

Example

The following example sets the configuration revision to 1.

```
switchxxxxxx(config) # spanning-tree mst configuration
switchxxxxxx(config-mst) # revision 1
```

29.26 show (MST)

Use the **show** MST Configuration mode command to display the current or pending MST region configuration.

Syntax

show ***{current*** | ***pending}***

Parameters

- **current**—Displays the current MST region configuration.
- **pending**—Displays the pending MST region configuration.

Default Configuration

N/A

Command Mode

MST Configuration mode

Example

The following example displays a pending MST region configuration

```
switchxxxxxx(config-mst)# show pending
Gathering information ..........
```

```
Current MST configuration
Name: Region1
Revision: 1
Instance  VLANs Mapped                State
--------  ------------------------    -----
0         1-4094                      Disabled
switchxxxxxx(config-mst)#
```

29.27 exit (MST)

Use the **exit** MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

Syntax
exit

Parameters
N/A

Default Configuration
N/A

Command Mode
MST Configuration mode

Example
The following example exits the MST Configuration mode and saves changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# exit
switchxxxxxx(config)#
```

29.28 abort (MST)

Use the **abort** MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

Syntax
abort

Parameters
N/A

Default Configuration
N/A

Command Mode
MST Configuration mode

Example
The following example exits the MST Configuration mode without saving changes.

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# abort
```

29.29 show spanning-tree
Use the **show spanning-tree** Privileged EXEC mode command to display the spanning-tree configuration.

Syntax
show spanning-tree *[interface-id] [**instance** instance-id]*

show spanning-tree *[**detail**] [**active** | **blockedports**] [**instance** instance-id]*

show spanning-tree ***mst-configuration***

Parameters
- **instance** *instance-id*—Specifies the spanning tree instance ID. (Range: 1–15)
- **detail**—Displays detailed information.
- **active**—Displays active ports only.
- **blockedports**—Displays blocked ports only.
- **mst-configuration**—Displays the MST configuration identifier.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
If no interface is specified, the default is all interfaces.

Command Mode
Privileged EXEC mode

User Guidelines
This command only works when MST is enabled.

Example

The following examples display spanning-tree information in various configurations:

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled

Root ID    Priority            32768
           Address             00:01:42:97:e0:00
           Cost                20000
           Port                fe1/0/11

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec


Bridge ID  Priority            36864
           Address             00:02:4b:29:7a:00

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec

Interfaces

Name       State    Prio. No    Cost    Sts     Role    PortFast Type
------     ------   ------      -----   ---     ----    -------- ----------
fe1/0/11   Enabled  128.1       20000   FWD     Root    No       P2p (RSTP)
fe1/0/12   Enabled  128.2       20000   FWD     Desg    No       Shared (STP)
fe1/0/13   Disabled 128.3       20000   -       -       -        -
fe1/0/14   Enabled  128.4       20000   BLK     Altn    No       Shared (STP)
fe1/0/15   Enabled  128.5       20000   DIS     -       -        -
```

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority            36864
           Address             00:02:4b:29:7a:00

           This switch is the Root.

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec

Interfaces
```

```
Name       State    Prio.Nbr    Cost    Sts     Role    PortFast Type
--------   -------- ---------   -----   ---     ----    -------- ----------
fe1/0/11   Enabled  128.1       20000   FWD     Desg    -        P2p (RSTP)
fe1/0/12   Enabled  128.2       20000   FWD     Desg    No       Shared (STP)
fe1/0/13   Disabled 128.3       20000   -       -       No       -
fe1/0/14   Enabled  128.4       20000   FWD     Desg    -        Shared (STP)
fe1/0/15   Enabled  128.5       20000   DIS     -       No       -
                                                        -
```

```
switchxxxxxx# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long

Root ID    Priority            N/A
           Address             N/A
           Path Cost           N/A
           Root Port           N/A
           Hello Time          N/A    Max Age N/A    Forward Delay N/A


Bridge ID  Priority            36864
           Address             00:02:4b:29:7a:00
           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec

Interfaces

Name       State    Prio.Nb     Cost    Sts     Role    PortFast Type
---------  -------- -------     -----   ---     ----    -------- ----------
fe1/0/11   Enabled  128.1       20000   -       -       -        -
fe1/0/12   Enabled  128.2       20000   -       -       -        -
fe1/0/13   Disabled 128.3       20000   -       -       -        -
fe1/0/14   Enabled  128.4       20000   -       -       -        -
fe1/0/15   Enabled  128.5       20000   -       -       -        -
                                                        -
```

```
switchxxxxxx# show spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority            32768
           Address             00:01:42:97:e0:00
           Path Cost           20000
           Root Port           fe1/0/11
           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec


Bridge ID  Priority            36864
           Address             00:02:4b:29:7a:00
           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec

Interfaces
```

```
Name       State    Prio.Nbr    Cost    Sts     Role    PortFast Type
---------  -------- ------      -----   ---     ----    -------- ----------
fe1/0/11   Enabled  128.1       20000   FWD     Root    -        P2p (RSTP)
fe1/0/12   Enabled  128.2       20000   FWD     Desg    No       Shared (STP)
fe1/0/14   Enabled  128.4       20000   BLK     Altn    No       Shared (STP)
                                                        No
```

```
switchxxxxxx# show spanning-tree blockedports
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority            32768
           Address             00:01:42:97:e0:00
           Path Cost           20000
           Root Port           fe1/0/11

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec


Bridge ID  Priority            36864

           Address             00:02:4b:29:7a:00

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec

Interfaces

Name       State    Prio.Nbr    Cost    Sts     Role    PortFast Type
---------  -------  ------      -----   ---     ----    -------- ----------
fe1/0/14   Enabled  128.4       19      BLK     Altn    No       Shared (STP)
```

```
switchxxxxxx# show spanning-tree detail
Spanning tree enabled mode RSTP
Default port cost method: long

Root ID    Priority            32768
           Address             00:01:42:97:e0:00
           Path Cost           20000
           Root Port           fe1/0/11

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec


Bridge ID  Priority            36864
           Address             00:02:4b:29:7a:00

           Hello Time 2 sec           Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 2d18h ago

Times:     hold 1, topology change 35, notification 2
           hello 2, max age 20, forward delay 15
```

```
Port 1 (fe1/0/11) enabled
State: Forwarding                       Role: Root
Port id: 128.1                          Port cost: 20000
Type: P2p (configured: auto) RSTP       Port Fast: No (configured:no)
Designated bridge Priority: 32768       Address: 00:01:42:97:e0:00
Designated port id: 128.25              Designated path cost: 0
Guard root: Disabled                    BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 2 (fe1/0/12) enabled
State: Forwarding                       Role: Designated
Port id: 128.2                          Port cost: 20000
Type: Shared (configured: auto) STP     Port Fast: No (configured:no)
Designated bridge Priority: 32768       Address: 00:02:4b:29:7a:00
Designated port id: 128.2               Designated path cost: 20000
Guard root: Disabled                    BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638

Port 3 (fe1/0/13) disabled
State: N/A                              Role: N/A
Port id: 128.3                          Port cost: 20000
Type: N/A (configured: auto)            Port Fast: N/A (configured:no)
Designated bridge Priority: N/A         Address: N/A
Designated port id: N/A                 Designated path cost: N/A
Guard root: Disabled                    BPDU guard: Disabled

Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A

Port 4 (fe1/0/14) enabled
State: Blocking                         Role: Alternate
Port id: 128.4                          Port cost: 20000
Type: Shared (configured:auto) STP      Port Fast: No (configured:no)
Designated bridge Priority: 28672       Address: 00:30:94:41:62:c8
Designated port id: 128.25              Designated path cost: 20000
Guard root: Disabled                    BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638

Port 5 (fe1/0/15) enabled
State: Disabled                         Role: N/A
Port id: 128.5                          Port cost: 20000
Type: N/A (configured: auto)            Port Fast: N/A (configured:no)
Designated bridge Priority: N/A         Address: N/A
Designated port id: N/A                 Designated path cost: N/A
Guard root: Disabled                    BPDU guard: Disabled

Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
```

```
switchxxxxxx# show spanning-tree ethernet fe1/0/11

Port 1 (fe1/0/11) enabled
State: Forwarding                       Role: Root
Port id: 128.1                          Port cost: 20000
Type: P2p (configured: auto) RSTP       Port Fast: No (configured:no)
Designated bridge Priority: 32768       Address: 00:01:42:97:e0:00
Designated port id: 128.25              Designated path cost: 0
Guard root: Disabled                    BPDU guard: Disabled

Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
```

```
switchxxxxxx# show spanning-tree mst-configuration
Name: Region1
Revision: 1

Instance            Vlans mapped        State
--------            ------------        ---------
0                   1-9, 21-4094        Enabled
1                   10-20               Enabled
```

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9

CST Root ID         Priority    32768
                    Address     00:01:42:97:e0:00
                    Path Cost   20000
                    Root Port    fe1/0/11

                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec


IST Master ID       Priority    32768
                    Address     00:02:4b:29:7a:00

                    This switch is the IST master.

                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec

                    Max hops 20


Interfaces

Name       State    Prio.Nbr    Cost    Sts     Role    PortFast Type
----       -------  --------    -----   ---     ----    -------- -------------
fe1/0/11   Enabled  128.1       20000   FWD     Root    No       P2p Bound
fe1/0/12   Enabled  128.2       20000   FWD     Desg    No       (RSTP)
fe1/0/13   Enabled  128.3       20000   FWD     Desg    No       Shared Bound
fe1/0/14   Enabled  128.4       20000   FWD     Desg    No       (STP)
                                                                 P2p
                                                                 P2p
```

```
###### MST 1 Vlans Mapped: 10-20

Root ID             Priority    24576
                    Address     00:02:4b:29:89:76
                    Path Cost   20000
                    Root Port    fe1/0/14
                    Rem hops    19


Bridge ID           Priority    32768
                    Address     00:02:4b:29:7a:00

Interfaces

Name       State    Prio.Nbr    Cost    Sts     Role    PortFast Type
----       -------  --------    -----   ---     ----    -------- --------------
fe1/0/11   Enabled  128.1       20000   FWD     Boun    No       P2p Bound
fe1/0/12   Enabled  128.2       20000   FWD     Boun    No       (RSTP)
fe1/0/13   Enabled  128.3       20000   BLK     Altn    No       Shared Bound
fe1/0/14   Enabled  128.4       20000   FWD     Root    No       (STP)
                                                                 P2p
                                                                 P2p
```

```
switchxxxxxx# show spanning-tree detail
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9

CST Root ID         Priority    32768
                    Address     00:01:42:97:e0:00
                    Path Cost   20000
                    Root Port    fe1/0/11

                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec


IST Master ID       Priority    32768
                    Address     00:02:4b:29:7a:00

                    This switch is the IST master.

                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec

                    Max hops 20
                    Number of topology changes 2 last change occurred 2d18h
                    ago
                    Times:  hold 1, topology change 35, notification 2
                    hello 2, max age 20, forward delay 15
```

```
Port 1 (fe1/0/11) enabled
State: Forwarding                               Role: Root
Port id: 128.1                                  Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP      Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:01:42:97:e0:00
Designated port id: 128.25                      Designated path cost: 0
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 2 (fe1/0/12) enabled
State: Forwarding                               Role: Designated
Port id: 128.2                                  Port cost: 20000
Type: Shared (configured: auto) Boundary STP    Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:7a:00
Designated port id: 128.2                       Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 3 (fe1/0/13) enabled
State: Forwarding                               Role: Designated
Port id: 128.3                                  Port cost: 20000
Type: Shared (configured: auto) Internal        Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:7a:00
Designated port id: 128.3                       Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 4 (fe1/0/14) enabled
State: Forwarding                               Role: Designated
Port id: 128.4                                  Port cost: 20000
Type: Shared (configured: auto) Internal        Port Fast: No (configured:no)
Designated bridge Priority: 32768               Address: 00:02:4b:29:7a:00
Designated port id: 128.2                       Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


###### MST 1 Vlans Mapped: 10-20

Root ID             Priority    24576
                    Address     00:02:4b:29:89:76
                    Path Cost   20000
                    Root Port    fe1/0/14

                    Rem hops 19


Bridge ID           Priority    32768
                    Address     00:02:4b:29:7a:00

                    Number of topology changes 2 last change occurred 1d9h
                    ago
```

```
                  Times:  hold 1, topology change 2, notification 2
                  hello 2, max age 20, forward delay 15


Port 1 (fe1/0/11) enabled
State: Forwarding                             Role: Boundary
Port id: 128.1                                Port cost: 20000
Type: P2p (configured: auto) Boundary RSTP    Port Fast: No (configured:no)
Designated bridge Priority: 32768             Address: 00:02:4b:29:7a:00
Designated port id: 128.1                     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638


Port 2 (fe1/0/12) enabled
State: Forwarding                             Role: Designated
Port id: 128.2                                Port cost: 20000
Type: Shared (configured: auto) Boundary STP  Port Fast: No (configured:no)
Designated bridge Priority: 32768             Address: 00:02:4b:29:7a:00
Designated port id: 128.2                     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 3 (fe1/0/13) disabled
State: Blocking                               Role: Alternate
Port id: 128.3                                Port cost: 20000
Type: Shared (configured: auto) Internal      Port Fast: No (configured:no)
Designated bridge Priority: 32768             Address: 00:02:4b:29:1a:19
Designated port id: 128.78                    Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638


Port 4 (fe1/0/14) enabled
State: Forwarding                             Role: Designated
Port id: 128.4                                Port cost: 20000
Type: Shared (configured: auto) Internal      Port Fast: No (configured:no)
Designated bridge Priority: 32768             Address: 00:02:4b:29:7a:00
Designated port id: 128.2                     Designated path cost: 20000
Number of transitions to forwarding state: 1
BPDU: sent 2, received 170638
```

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9

CST Root ID        Priority    32768
                   Address     00:01:42:97:e0:00
                   Path Cost   20000
                   Root Port    fe1/0/11
```

```
                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec

IST Master ID       Priority    32768
                    Address     00:02:4b:19:7a:00
                    Path Cost   10000
                    Rem hops    19

Bridge ID           Priority    32768
                    Address     00:02:4b:29:7a:00
                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec
                    Max hops 20
```

```
switchxxxxxx# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9
CST Root ID         Priority    32768
                    Address     00:01:42:97:e0:00
                    This switch is root for CST and IST master.
                    Root Port    fe1/0/11
                    Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec
                    Max hops 20
```

29.30 show spanning-tree bpdu

Use the **show spanning-tree bpdu** EXEC mode command to display the BPDU handling when spanning-tree is disabled.

Syntax

show spanning-tree bpdu *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example
The following examples display spanning-tree BPDU information:

```
switchxxxxxx# show spanning-tree bpdu

The following is the output if the global BPDU handling
command is not supported.

Interface       Admin Mode      Oper Mode
---------       ----------      ---------
fe1/0/11        Filtering       Filtering
fe1/0/12        Filtering       Filtering
fe1/0/13        Filtering       Guard

The following is the output if both the global BPDU
handling command and the per-interface BPDU handling
command are supported.

Global: Flooding


Interface       Admin Mode      Oper Mode
---------       ----------      ---------
fe1/0/11        Global          Flooding
fe1/0/12        Global          STP
fe1/0/13        Flooding        STP
```

29.31 spanning-tree loopback-guard
Use the **spanning-tree loopback-guard global configuration** command to shut down an interface if it receives a loopback BPDU. Use the **no** form of this command to return the default setting.

Syntax
spanning-tree loopback-guard

no spanning-tree loopback-guard

Parameters
N/A

Default Configuration
N/A

Command Mode
Global

User Guidelines
This enables shutting down all interfaces if a loopback BPDU is received on it.

Example

```
switchxxxxxx(config)# spanning-tree loopback-guard
```

30 Virtual Local Area Network (VLAN) Commands

30.1 vlan database

Use the **vlan database** Global Configuration mode command to enter the VLAN Configuration mode. This mode is used to create VLAN(s) and define the default VLAN.

Use the **exit** command to return to Global Configuration mode.

Syntax

vlan database

Parameters

N/A

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

Example

The following example enters the VLAN Configuration mode, creates VLAN 1972 and exits VLAN Configuration mode.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 1972
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)#
```

30.2 vlan

Use the **vlan** VLAN Configuration mode or Global Configuration mode command to create a VLAN and assign it a name (if only a single VLAN is being created). Use the **no** form of this command to delete the VLAN(s).

Syntax

vlan *vlan-range*

no vlan *vlan-range*

Parameters

- **vlan-range**—Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 2-4094).

- **name**—Specifies the VLAN name. The option is only valid where only one VLAN is configured by the command (range: 1–32 characters).

Default Configuration
VLAN 1 exists by default.

Command Mode
Global Configuration mode

VLAN Configuration mode

Example
The following example creates VLAN number 1972 and assigns it the name Marketing.

```
switchxxxxxx(config)#vlan database
switchxxxxxx(config-vlan)#vlan 1972 Marketing
switchxxxxxx(config-vlan)#
```

30.3 show vlan
Use the **show vlan** Privileged EXEC mode command to display the following VLAN information for all VLANs or for a specific VLAN:

- VLAN ID
- VLAN name
- Ports on the VLAN
- Whether the VLAN was is dynamic or permanent
- Whether authorization is required on the VLAN

Syntax
show vlan [***tag*** *vlan-id* | ***name*** *vlan-name*]

Parameters
- **tag** *vlan-id*—Specifies a VLAN ID.
- **name** *vlan-name*—Specifies a VLAN name string (length: 1–32 characters)

Default Configuration
All VLANs are displayed.

Command Mode
Privileged EXEC mode

Examples:

Example 1 - The following example displays information for all VLANs:.

```
switchxxxxxx# show vlan

VLAN   Name         Ports          Type         Authorization
----   ---------    --------       -------      -------------
1      default      fe1/0/11-2     Default      Required
10     Marketing    fe1/0/13-14    Static       Required
11     VLAN0011     fe1/0/15-16    Static       Required
20     VLAN0020     fe1/0/17-18    Static       Required
21     VLAN0021                    Static       Required
30     VLAN0030                    Static       Required
31     VLAN0031                    Static       Required
91     VLAN0091     fe1/0/12       Dynamic      Not Required
3978   Guest        fe1/0/17       Static       Guest
       VLAN
```

Example 2 - The following example displays information for the default VLAN (VLAN 1):

```
switchxxxxxx# show vlan tag default

VLAN   Name         Ports          Type        Authorization
----   ---------    --------       -------     -------------
1      default      fe1/0/11-2     Default     Required
```

Example 3 - The following example displays information for the VLAN named Marketing:

```
switchxxxxxx# show vlan name Marketing

VLAN   Name         Ports          Type        Authorization
----   ---------    --------       -------     -------------
1      Marketing    fe1/0/13-14    static      Required
```

30.4 show default-vlan-membership

Use the **show default-vlan-membership** privileged EXEC command to view the default VLAN membership.

Syntax

show default-vlan-membership [*interface-id*]

Parameters

interface-id—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel

Default Configuration

Membership in the default VLAN is displayed for all interfaces.

Command Mode

Privileged EXEC

Example

```
switchxxxxxx # show default-vlan-membership

Port    Forbidden     Membership
----    ------        -------
fe1/0/11    TRUE          FALSE
fe1/0/12    FALSE         TRUE
fe1/0/13    FALSE         FALSE
```

30.5 interface vlan

Use the **interface vlan** Global Configuration mode command to enter the Interface Configuration (VLAN) mode for a specific VLAN. After this command is entered, all commands configure this VLAN. To configure a range of VLANs, use **interface range vlan**.

Syntax

interface vlan *vlan-id*

Parameters

vlan *vlan-id*—Specifies the VLAN to be configured.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

If the VLAN does not exist (ghost VLAN), some commands are not available under the interface VLAN context.

The commands that are supported for VLANs but do not exist for ghost VLANs are:

- IGMP snooping control commands
- Bridge Multicast configuration commands

Example
The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
switchxxxxxx (config)# interface vlan 1
switchxxxxxx (config-if)# ip address 131.108.1.27 255.255.255.0
```

30.6 interface range vlan
Use the **interface range vlan** Global Configuration mode command to configure multiple VLANs simultaneously.

Syntax
interface range vlan *vlan-range*

Parameters
vlan *vlan-range*—Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

Default Configuration
N/A

Command Mode
Global Configuration mode

User Guidelines
Commands under the interface VLAN range context are executed independently on each VLAN in the range. If the command returns an error on one of the VLANs, an error message is displayed, and the system attempts to configure the remaining VLANs.

If a VLAN does not exist (ghost VLAN), some commands are not available under the interface VLAN context. These are:

- IGMP snooping control commands
- Bridge Multicast configuration commands

Example
The following example groups VLANs 221 through 228 and 889 to receive the same command(s).

```
switchxxxxxx(config)# interface range vlan 221-228, vlan 889
switchxxxxxx(config-if)#
```

30.7 name
Use the **name** Interface Configuration (VLAN) mode command to name a VLAN. Use the **no** form of this command to remove the VLAN name.

Syntax
name *string*

no name

Parameters
string—Specifies a unique name associated with this VLAN. (Length: 1–32 characters)

Default Configuration
No name is defined.

Command Mode
Interface Configuration (VLAN) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
The VLAN name must be unique.

Example
The following example assigns VLAN 19 the name Marketing.

```
switchxxxxxx(config)# interface vlan 19
switchxxxxxx(config-if)# name Marketing
```

30.8 switchport protected-port
Use the **switchport protected-port** Interface Configuration mode command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

Syntax
switchport protected-port

no switchport protected-port

Parameters
N/A

Default Configuration
Unprotected

Command Mode
Interface configuration (Ethernet, port-channel)

User Guidelines
Note that packets are subject to all filtering rules and Filtering Database (FDB) decisions.

Use this command to isolate Unicast, Multicast, and Broadcast traffic at Layer 2 from other protected ports (that are not associated with the same community as the ingress interface) on the same switch. Please note that the packet is still subject to FDB decision and to all filtering rules. Use the **switchport community** Interface Configuration command to associate the interface with a community.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport protected-port
```

30.9 show interfaces protected-ports

Use the **show interfaces protected-ports** EXEC mode command to display protected ports configuration.

Syntax

show interfaces protected-ports [*interface-id*]

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

Show all protected ports.

Command Mode

EXEC mode

Example

```
switchxxxxxx# show interfaces protected-ports

Interface     State      Community
--------- -------------  ---------
  fe1/0/11      Protected       1
  fe1/0/12      Protected       Isolated
  fe1/0/13      Unprotected     20
  fe1/0/14      Unprotected     Isolated
```

Note: The Community column for unprotected ports is relevant only when the port state is changed to Protected.<gina - not clear why is there community for unprotected ports?>

30.10 switchport community

Use the **switchport community** Interface Configuration mode command to associate a protected port with a community. Use the **no** form of this command to return to the default.

Syntax

switchport community *community*

no switchport community

Parameters
community *community*—Specifies the community number. (range: 1 - 30)

Default Configuration
The port is not associated with a community.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The command is relevant only when the port is defined as a protected port. Use the s**witchport protected-port** Interface Configuration command to define a port as a protected port.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport community 1
```

30.11 switchport
Use the **switchport** Interface Configuration mode command to put an interface that is in Layer 3 mode into Layer 2 mode. Use the **no** form of this command to put an interface in Layer 3 mode.

Syntax
switchport

no switchport

Parameters
N/A

Default Configuration
Layer 2 mode

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Examples:

Example 1 - The following example puts the port gi1 into Layer 2 mode.

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)#switchport
```

Example 2 - The following example puts the port gi1 into Layer 3 mode.

```
switchxxxxxx(config)# interface gi1
```

```
switchxxxxxx(config-if)#no switchport
```

30.12 switchport mode

Use the **switchport mode** Interface Configuration (Ethernet, port-channel) mode command to configure the VLAN membership mode (access, trunk, general or customer) of a port. Use the **no** form of this command to restore the default configuration.

Syntax

switchport mode ***{access*** | ***trunk*** | ***general*** | ***customer}***

no switchport mode

Parameters

- **access**—Specifies an untagged layer 2 VLAN port.
- **trunk**—Specifies a trunking layer 2 VLAN port.
- **general**—Specifies a full 802-1q-supported VLAN port.
- **customer**—Specifies that the port is connected to customer equipment. Used when the switch is in a provider network.

Default Configuration

Access mode.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

- When the port's mode is changed, it receives the configuration corresponding to the mode.
- If the port mode is changed to access and the access VLAN does not exist, then the port does not belong to any VLAN.
- Trunk and general mode ports can be changed to access mode only if all VLANs (except for an untagged PVID are first removed.

Example

The following example configures `fe1/0/11` as an access port (untagged layer 2) VLAN port.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

30.13 switchport access vlan

A port in access mode can be an untagged member of at most a single VLAN. The **switchport access vlan** Interface Configuration command reassigns an interface to a different VLAN than it currently belongs or assigns it to *none*, in which case it is not a member of any VLAN.

The **no** form of this command to restore the default configuration.

Syntax

switchport access vlan *{vlan-id* | ***none}***

no switchport access vlan

Parameters

vlan *vlan-id*—Specifies the VLAN to which the port is configured.

vlan ***none***—Specifies that the access port cannot belong to any VLAN.

Default Configuration

The interface belongs to the default VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

When the port is assigned to a different VLAN, it is automatically removed from its previous VLAN and added it to the new VLAN. If the port is assigned to *none,* it is removed from the previous VLAN and not assigned to any other VLAN.

Example

The following example assigns access port gi1 to VLAN 2 (and removes it from its previous VLAN).

```
switchxxxxxx(config)# interface fe1/0/12
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

30.14 switchport trunk allowed vlan

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. Use the **switchport trunk allowed vlan** Interface Configuration mode command to add/remove VLAN(s) to/from a trunk port.

Syntax

switchport trunk allowed vlan ***{all*** | ***none*** | ***add*** *vlan-list* | ***remove*** *vlan-list* | ***except*** *vlan-list}*

Parameters

all—Specifies all VLANs from 1 to 4094. At any time, the port belongs to all VLANs existing at the time. (range: 1–4094)

none—Specifies an empty VLAN list The port does not belong to any VLAN.

add *vlan-list*—List of VLAN IDs to add to the port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

remove *vlan-list*—List of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

except *vlan-list*—List of VLAN IDs is calculated by inverting the defined list of VLANs (the calculated list will include all VLANs from 1 - 4094 except VLANs from the this list.

Default Configuration
By default, trunk ports belongs to all created VLANs.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
Inside **except except-vlan-list** is saved as **add ~ vlan-list**, where **~ vlan-list** is a list of all VLANs from 1 to 4094 minus the VLANs from **except-vlan-list**. The **show running/startup** command always uses the latter format.

The port must be in trunk mode before the command can take effect.

Example
To add VLANs 2,3 and 100 to trunk ports 1 to 13

```
switchxxxxxx(config)# interface range fe1/0/11-13
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
switchxxxxxx(config-if)#
```

30.15 switchport trunk allowed vlan
A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. The **switchport trunk allowed vlan** Interface Configuration mode command adds/removes VLAN(s) to/from a trunk port.

Syntax
switchport trunk allowed vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters
- **add** *vlan-list* — Specifies a list of VLAN IDs to add to a port. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **remove** *vlan-list* — Specifies a list of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

Default Configuration
By default, trunk ports belongs to all created VLANs.

Command Mode
Interface Configuration (Ethernet, port-channel) mode

Example
To add VLANs 2,3 and 100 to trunk ports 1 to 13:

```
switchxxxxxx(config)# interface range fe1/0/11-13
switchxxxxxx(config-if)# switchport mode trunk
```

```
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
switchxxxxxx(config-if)#
```

30.16 switchport trunk native vlan

If an untagged packet arrives on a trunk port, it is directed to the port's native VLAN. Use the **switchport trunk native vlan** Interface Configuration (Ethernet, port-channel) mode command to define the native VLAN for a trunk interface. Use the **no** form of this command to restore the default native VLAN.

Syntax

switchport trunk native vlan *{vlan-id* | ***none}***

no switchport trunk native vlan

Parameters

- **vlan-id**—Specifies the native VLAN ID.
- **none**—Specifies the access port cannot belong to any VLAN.

Default Configuration

If the default VLAN is enabled, the default native VLAN is 1. Otherwise, the default native VLAN is 4095.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command adds the port as a member of the VLAN. If the port is already a member of the VLAN (not a native), it must first be removed from the VLAN.

Examples:

Example 1 - The following example:

- Defines VLAN 2 as native VLAN for port 1
- Removes VLAN 2 from port 1 and then sets it as the native VLAN

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport trunk native vlan 2
Port 1: Port is Trunk in VLAN 2.
switchxxxxxx(config-if)# switchport trunk allowed vlan remove 2
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)#
```

Example 2 - The following example sets packets on port as untagged on ingress and untagged on egress:

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport mode trunk
```

```
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)#
```

Example 3 - The following example sets packets on port are tagged on ingress and tagged on egress:

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2
switchxxxxxx(config-if)#
```

30.17 switchport general allowed vlan

General ports can receive tagged or untagged packets. Use the **switchport general allowed vlan** Interface Configuration mode command to add/remove VLANs to/from a general port and configure whether packets on the egress are tagged or untagged. Use the **no** form of this command to reset to the default.

Syntax

switchport general allowed vlan *{***add** | **remove***}* *vlan-list [***tagged** | **untagged***]*

no switchport general allowed vlan

Parameters

- **add** *vlan-list*—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. (range: 1–4094)
- **remove** *vlan-list*—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **tagged**—Specify that packets are transmitted tagged for the configured VLANs
- **untagged**—Specify that packets are transmitted untagged for the configured VLANs (this is the default)

Default Configuration

The port is not a member of any VLAN.

Packets are transmitted untagged.

Command Mode

Interface Configuration mode

Example

Sets port 1 to general mode and adds VLAN 2 and 3 to it. Packets are tagged on the egress.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

30.18 switchport general allowed vlan

General ports can receive tagged or untagged packets. Use the **switchport general allowed vlan** Interface Configuration mode command to add/remove VLANs to/from a general port and configure whether packets on the egress are tagged or untagged. Use the **no** form of this command to reset to the default.

Syntax

switchport general allowed vlan {[**add** *vlan-list* [***tagged*** | ***untagged***]] | [***remove*** *vlan-list*]}

Parameters

- **add** *vlan-list* — Specifies the list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.
- **tagged** — Specifies that the port transmits tagged packets for the VLANs. This is the default value
- **untagged** — Specifies that the port transmits untagged packets for the VLANs.
- **remove** *vlan-list* — Specifies the list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs.

Default Configuration

The port is not member in any VLAN.

Packets are transmitted untagged.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

You can change the egress rule (for example, from tagged to untagged) without first removing the VLAN from the list.

Example

Sets port 1 to general mode and adds VLAN 2 and 3 to it. Packets are tagged on the egress.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

30.19 switchport general pvid

The port VLAN ID (PVID) is the VLAN to which incoming untagged and priority-tagged frames are classified on a general port. Use the **switchport general pvid** Interface Configuration (Ethernet, Port-channel) mode command to configure the Port VLAN ID (PVID) of an interface when it is in general mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport general pvid *vlan-id*

no switchport general pvid

Parameters

pvid *vlan-id*—Specifies the Port VLAN ID (PVID).

Default Configuration

The default VLAN is the PVID.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

Example 1 - The following example configures port 2 as a general port and sets its PVID to 234.

```
switchxxxxxx(config)# interface fe1/0/12
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general pvid 234
```

Example 2 - Performs the following:

- Adds VLANs 2&3 as tagged, and VLAN 100 as untagged to general mode port 14
- Defines VID 100 as the PVID
- Reverts to the default PVID (VID=1)

```
switchxxxxxx(config)# interface fe1/0/114
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)#  switchport general allowed vlan add 2-3
tagged
switchxxxxxx(config-if)# switchport general allowed vlan add 100
untagged
switchxxxxxx(config-if)# switchport general pvid 100
switchxxxxxx(config-if)# no switchport general pvid
switchxxxxxx(config-if)#
```

Example 3 - Configures VLAN on port 14 as untagged on input and untagged on output:

```
switchxxxxxx(config)# interface fe1/0/114
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)#  switchport general pvid 2
switchxxxxxx(config-if)# switchport general allowed vlan add 2 untagged
switchxxxxxx(config-if)#
```

Example 4 - Configures VLAN on port 21 as untagged on input and tagged on output:

```
switchxxxxxx(config)# interface fe1/0/121
```

```
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)#  switchport general pvid 2
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)#
```

Example 5 - Configures VLAN on port 14 as tagged on input and tagged on output:

```
switchxxxxxx(config)# interface fe1/0/114
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)#
```

Example 6 - Configures VLAN on port 23 as tagged on input and untagged on output:

```
switchxxxxxx(config)# interface fe1/0/123
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)#
```

30.20 switchport general ingress-filtering disable

Use the **switchport general ingress-filtering disable** Interface Configuration (Ethernet, Port-channel) mode command to disable port ingress filtering (no packets are discarded at the ingress) on a general port. Use the no form of this command to restore the default configuration.

Syntax

switchport general ingress-filtering disable

no switchport general ingress-filtering disable

Parameters

N/A

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example disables port ingress filtering on `fe1/0/11`.

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

30.21 switchport general acceptable-frame-type

The **switchport general acceptable-frame-type** Interface Configuration mode command configures the types of packets (tagged/untagged) that are filtered (discarded) on the interface. Use the **no** form of this command to return ingress filtering to the default.

Syntax

switchport general acceptable-frame-type ***{tagged-only*** | ***untagged-only*** | ***all}***

no switchport general acceptable-frame-type

Parameters

- **tagged-only**—Ignore (discard) untagged packets and priority-tagged packets.
- **untagged-only**—Ignore (discard) VLAN-tagged packets (not including priority-tagged packets)
- **all**—Do not discard packets untagged or priority-tagged packets.

Default Configuration

All frame types are accepted at ingress (**all**).

Command Mode

Interface Configuration (Ethernet, port-channel) mode

Example

The following example configures port `fe1/0/13` to be in general mode and to discard untagged frames at ingress.

```
switchxxxxxx(config)# interface fe1/0/13
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type
tagged-only
```

30.22 switchport customer vlan

When a port is in customer mode it is in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across a provider network. The switch is in QinQ mode when it has one or more customer ports.

Use the **switchport customer vlan** Interface Configuration mode command to set the port's VLAN when the interface is in customer mode (set by switchport mode). Use the no form of this command to restore the default configuration.

Syntax

switchport customer vlan *vlan-id*

no switchport customer vlan

Parameters

vlan *vlan-id*—Specifies the customer VLAN.

Default Configuration
No VLAN is configured as customer.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example defines `fe1/0/15` as a member of customer VLAN 5.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

30.23 map protocol protocols-group
Forwarding of packets based on their protocol requires setting up groups of protocols and then mapping these groups to VLANs. Use the **map protocol protocols-group** VLAN Configuration mode command to map a protocol to a group of protocols. This protocol group can then be used in switchport general map protocols-group vlan. Use the **no** form of this command to delete a protocol from a group.

Syntax
map protocol *protocol* [***encapsulation***] **protocols-group** *group*

no map protocol *protocol* [*encapsulation*]

Parameters
- **protocol**—Specifies a 16-bit protocol number or one of the reserved names listed in the User Guidelines. (range: 0x0600–0xFFFF)
- **encapsulation**—Specifies one of the following values: Ethernet, rfc1042, llcOther.
- **protocols-group** *group*—Specifies the group number of the group of protocols (range: 1–2147483647).

Default Configuration
The default encapsulation is Ethernet.

Command Mode
VLAN Configuration mode

User Guidelines
The value 0x8100 is not valid as the protocol number for Ethernet encapsulation.

The following protocol names are reserved for Ethernet Encapsulation:

- ip
- arp
- ipv6
- ipx

Example
The following example maps the IP protocol to protocol group number 213.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map protocol ip protocols-group 213
```

30.24 switchport general map protocols-group vlan
Use the **switchport general map protocols-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to forward packets based on their protocol, otherwise known as setting up a classifying rule. This command forwards packets arriving on an interface containing a specific protocol to a specific VLAN.

Use the no form of this command to stop forwarding packets based on their protocol.

Syntax
switchport general map protocols-group *group* **vlan** *vlan-id*

no switchport general map protocols-group *group*

Parameters
- **group**—Specifies the group number as defined in map protocol protocols-group (range: 1–65535).
- **vlan** *vlan-id*—Defines the VLAN ID in the classifying rule.

Default Configuration
N/A

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
The VLAN classification rule priorities are:

4. MAC-based VLAN (best match among the rules)
5. Subnet-based VLAN (best match among the rules)
6. Protocol-based VLAN
7. PVID

Example
The following example forwards packets with protocols belong to protocol-group 1 to VLAN 8.

```
switchxxxxxx(config-if)# switchport general map protocols-group 1 vlan
8
```

30.25 show vlan protocols-groups
Use the **show vlan protocols-groups** EXEC mode command to display the protocols that belong to the defined protocols-groups.

Syntax
show vlan protocols-groups

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example displays protocols-groups information.

```
switchxxxxxx# show vlan protocols-groups

Protocol              Encapsulation         Group
-------------         --------------        --------
0x800 (IP)            Ethernet              1
0x806 (ARP)           Ethernet              1
0x86dd (IPv6)         Ethernet              2
0x8898                Ethernet              3
```

30.26 map mac macs-group
Forwarding of packets based on their MAC address requires setting up groups of MAC addresses and then mapping these groups to VLANs.

Use the **map mac macs-group** VLAN Configuration mode command to map a MAC address or range of MAC addresses to a group of MAC addresses, which is then used in switchport general map macs-group vlan. Use the **no** form of this command to delete the mapping.

This command can only be used when the device is in Layer 2 mode.

Syntax
map mac *mac-address* {*prefix-mask* | ***host***} ***macs-group*** *group*

no map mac *mac-address* {*prefix-mask* | ***host***}

Parameters
- **mac** *mac-address*—Specifies the MAC address to be mapped to the group of MAC addresses.
- **prefix-mask**—Specifies the number of ones in the mask.
- **host**—Specifies that the mask is comprised of all 1s.
- **macs-group** *group*—Specifies the group number (range: 1–2147483647)

Default Configuration
N/A

Command Mode
VLAN Configuration mode

Example
The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface fe1/0/111
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

30.27 switchport general map macs-group vlan
After groups of MAC addresses have been created (see map mac macs-group), they can be mapped to specific VLANs.

Use the **switchport general map macs-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to set a MAC-based classification rule. Use the no form of this command to delete a classification rule.

Syntax
switchport general map macs-group *group* **vlan** *vlan-id*

no switchport general map macs-group *group*

Parameters
- **macs-group** *group*—Specifies the group number (range: 1–2147483647)
- **vlan** *vlan-id*—Defines the VLAN ID associated with the rule.

Default Configuration
N/A

Command Mode
Interface Configuration (Ethernet, port-channel) mode

User Guidelines
MAC-based VLAN rules cannot contain overlapping ranges on the same interface.

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules).
2. Subnet-based VLAN (Best match among the rules).
3. Protocol-based VLAN.
4. PVID.

Example

The following example creates two groups of MAC addresses, sets a port to general mode and maps the groups of MAC addresses to specific VLANs.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# map mac 0000.1111.0000 32 macs-group 1
switchxxxxxx(config-vlan)# map mac 0000.0000.2222 host macs-group 2
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# interface fe1/0/111
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general map macs-group 1 vlan 2
switchxxxxxx(config-if)# switchport general map macs-group 2 vlan 3
```

30.28 show vlan macs-groups

Use the **show vlan macs-groups** EXEC mode command to display the MAC addresses that belong to the defined MACs-groups.

Syntax

show vlan macs-groups

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays macs-groups information.

```
switchxxxxxx# show vlan macs-groups

     MAC Address              Mask                Group ID
--------------------- --------------------- ---------------------
  00:12:34:56:78:90            20                    22
  00:60:70:4c:73:ff            40                    1
```

30.29 map subnet subnets-group

Forwarding of packets based on their IP subnet requires setting up groups of IP subnets and then mapping these groups to VLANs. Use the **map subnet subnets-group** VLAN Configuration mode command to map an IP subnet to a group of IP subnets. Use the **no** form of this command to delete the map.

Syntax

map subnet *ip-address prefix-mask* **subnets-group** *group*

no map subnet *ip-address prefix-mask*

Parameters

- **ip-address**—Specifies the IP address prefix of the subnet to be mapped to the group.
- **prefix-mask**—Specifies the number of 1s in the mask.
- **subnets-group** *group*—Specifies the group number. (range: 1–2147483647)

Default Configuration

N/A

Command Mode

VLAN Configuration mode

Example

The following example maps an IP subnet to the group of IP subnets 4. It then maps this group of IP subnets to VLAN 8

```
switchxxxxxx(config)#vlan database
switchxxxxxx(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
switchxxxxxx(config-if)# switchport general map subnets-group 4 vlan 8
```

30.30 switchport general map subnets-group vlan

Use the **switchport general map subnets-group vlan** Interface Configuration (Ethernet, Port-channel) mode command to set a subnet-based classification rule. Use the **no** form of this command to delete a subnet-based classification rule.

Syntax

switchport general map subnets-group *group* **vlan** *vlan-id*

no switchport general map subnets-group *group*

Parameters

- **group**—Specifies the group number. (range: 1–2147483647)
- **vlan-id**—Defines the VLAN ID associated with the rule.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The VLAN classification rule priorities are:

1. MAC-based VLAN (Best match among the rules)

2. Subnet-based VLAN (Best match among the rules)
3. Protocol-based VLAN
4. PVID

Example
The following example maps an IP subnet to the group of IP subnets 4. It then maps this group of IP subnets to VLAN 8

```
switchxxxxxx(config)#vlan database
switchxxxxxx(config-vlan)# map subnet 172.16.1.1 24 subnets-group 4
switchxxxxxx(config-if)# switchport general map subnets-group 4 vlan 8
```

30.31 show vlan subnets-groups
Use the **show vlan subnets-groups** EXEC mode command to display subnets-groups information.

Syntax
show vlan subnets-groups

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example displays subnets-groups information.

```
switchxxxxxx# show vlan subnets-groups

IP Subnet Address    Mask        Group ID
---------------- ----------- --------------
     1.1.1.1          32            1
   172.16.2.0         24            2
```

30.32 switchport forbidden default-vlan
Use the **switchport forbidden default-vlan** Interface Configuration command to forbid a port from being added to the default VLAN. Use the no form of this command to revert to default.

Syntax
switchport forbidden default-vlan

no switchport forbidden default-vlan

Parameters
N/A

Default Configuration
Membership in the default VLAN is allowed.

Command Mode
Interface and Interface range configuration (Ethernet, port-channel)

User Guidelines
The command may be used at any time regardless of whether the port belongs to the default VLAN.

The **no** command does not add the port to the default VLAN, it only defines an interface as permitted to be a member of the default VLAN, and the port will be added only when conditions are met.

Example

The following example forbids the port gi1 from being added to the default VLAN.

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)# switchport forbidden default-vlan
```

30.33 switchport forbidden vlan

The **switchport forbidden vlan** Interface Configuration (Ethernet, Port-channel) mode command forbids adding or removing specific VLANs to or from a port. To restore the default configuration, use the **no** form of this command.

Syntax
switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

no switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

Parameters
- **add** *vlan-list* — Specifies a list of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen designate a range of IDs.
- **remove** *vlan-list* — Specifies a list of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen designate a range of IDs.

Default Configuration
All VLANs are allowed.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example forbids adding VLAN IDs 234 to 256 to `fe1/0/17`.

```
switchxxxxxx(config)# interface fe1/0/17
```

```
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport forbidden vlan add 234-256
```

30.34 switchport default-vlan tagged

Use the **switchport default-vlan tagged** Interface Configuration command to configure the port as a tagged port in the default VLAN. Use the **no** form of the command to return the port to an untagged port.

Syntax

switchport default-vlan tagged

no switchport default-vlan tagged

Parameters

N/A

Default Configuration

If the port is a member in the default VLAN, by default, it is a member as an untagged port.

Command Mode

Interface configuration (Ethernet, port-channel)

User Guidelines

The command adds a port to the default VLAN as a tagged port.

The command is available only if the port mode is trunk or general.

When a trunk port is a member in the default VLAN as a tagged port then:

- The native VLAN cannot be the default VLAN
- The default of the native VLAN is 4095

Note: If the native VLAN of a port is the default VLAN when the port is added to the default VLAN as tagged, the native VLAN is set by the system to 4095.

When a general port is a member in the default VLAN as a tagged port then:

- The PVID can be the default VLAN.
- The default PVID is the default VLAN.

Note: The PVID is not changed when the port is added to the default VLAN as a tagged.

When executing the **switchport default-vlan tagged** command, the port is added (automatically by the system) to the default VLAN when the following conditions no longer exist:

- The port is a member in a LAG.
- The port is 802.1X unauthorized.
- An IP address is defined on the port.
- The port is a destination port of port mirroring.
- An IP address is defined on the default VLAN and the port is a PVE protected port.

The **no switchport default-vlan tagged** command removes the port from the default VLAN, and returns the default VLAN mode to untagged.

Note:

- If the native VLAN of a trunk port is 4095 when the port is removed from the default VLAN (as a tagged), the native VLAN is set by the system to the default VLAN.

- The PVID of a general port is not changed when the port is removed from the default VLAN (as a tagged). If the PVID is the default VLAN, the port is added by the system to the default VLAN as an untagged.

Example
The following example configures the port fe1/0/11 as a tagged port in the default VLAN.

```
switchxxxxxx(config)#interface gi1
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)#switchport default-vlan tagged
```

30.35 show interfaces switchport
Use the **show interfaces switchport** Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

Syntax
show interfaces switchport *[interface-id]*

Parameters
interface-id—Specify an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel

Default Configuration
Displays information for all interfaces.

Command Mode
EXEC mode

Examples:

Example 1 - The following example displays the the command output for a trunk port:

```
switchxxxxxx# show interfaces switchport fe1/0/11
Port fe1/0/11:
Port Mode: Trunk
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 2
Protected: Enabled, Uplink is fe1/0/19.
Port fe1/0/11 is member in:
    VLAN   Name          Egress Rule  Type
    ----   ----------    ----------- -----
    1      default       untagged    System
    8       VLAN008       tagged      Dynamic
```

```
   11      VLAN0011      tagged      Static
   19       IPv6VLAN      untagged    Static
   72       VLAN0072      untagged    Static
Forbidden VLANS:
    VLAN     Name
    ----     ---------
    73       Out
Classification rules:
Mac based VLANs:
  Group ID   Vlan ID
```

Example 2 - The following example displays the output for a general port:

```
switchxxxxxx# show interfaces switchport fe1/0/12
Port fe1/0/12:
VLAN Membership mode: General
Operating Parameters:
PVID: 4095 (discard vlan)
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
Protected: Disabled
Port fe1/0/11 is member in:
VLAN   Name         Egress Rule Type
----   ---------    ----------- -----
91     IP Telephony   tagged    Static
Protected: Disabled
Port fe1/0/12 is statically configured to:
VLAN   Name            Egress Rule Type
----   ---------       ----------- -----
8       VLAN0072        untagged
91     IP Telephony     tagged
Forbidden VLANS:
VLAN   Name
----   ---------
73      Out
```

Example 3 - The following example displays the command output for an access port:

```
switchxxxxxx# show interfaces switchport fe1/0/12
Port fe1/0/12:
Port Mode: Access
```

```
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 1
Port is member in:
Vlan               Name               Egress Rule Port Membership Type
---- -------------------------------- ----------- --------------------
 1                  1                  Untagged          System
Forbidden VLANS:
Vlan               Name
---- --------------------------------
Classification rules:
Mac based VLANs:
```

30.36 show interfaces switchport

Use the **show interfaces switchport** Privileged EXEC command to display the administrative and operational status of all interfaces or a specific interface.

Syntax

show interfaces switchport *[interface-id]*

Parameters

Interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ehernet port or Port-channel.

Command Mode

Privileged EXEC mode

Default

Displays the status of all interfaces.

Example

```
switchxxxxxx# show interfaces switchport fe1/0/11

Protected: Enabled, Uplink is fe1/0/11
Classification rules:
Classification Type   Group ID   VLAN ID
-------------------   --------   -------
Protocol                   1        19
Protocol                   1        20
Protocol                   2        72
Subnet                     1        15
MAC                        6        11
```

30.37 ip internal-usage-vlan

The system assigns a VLAN to every IP address. In rare cases, this might conflict with a user requirement for that VLAN. In this case, use the **ip internal-usage-vlan** Interface Configuration (Ethernet, Port-channel) mode command to reserve a different VLAN as the internal usage VLAN of an interface. Use the **no** form of this command to restore the default configuration.

Syntax

ip internal-usage-vlan *vlan-id*

no ip internal-usage-vlan

Parameters

vlan-id—Specifies the internal usage VLAN ID.

Default Configuration

No VLAN is reserved as an internal usage VLAN by default (using this command).

Command Mode

Interface Configuration (Ethernet, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

An internal usage VLAN is assigned by the system when an IP interface is defined on an Ethernet port or port-channel.

If an internal usage VLAN is not defined for a port, the software selects one of the unused VLANs.

If a VLAN was chosen by the software for internal usage, but you want to use that VLAN for a static or dynamic VLAN, do one of the following:

- Remove the IP address from the interface (this releases the internal usage VLAN).
- Recreate the VLAN on the required interface (now it will be assigned to the interface and not be used as an internal usage VLAN)
- Recreate the IP interface (another internal usage VLAN is assigned to this IP interface) or use this command to explicitly define the internal usage VLAN.

Example

The following example reserves unused VLAN 200 as the internal usage VLAN of `fe1/0/13`.

```
switchxxxxxx(config)# interface fe1/0/13
switchxxxxxx(config-if)# ip internal-usage-vlan 200
```

30.38 show vlan internal usage

Use the **show vlan internal usage** Privileged EXEC mode command to display a list of VLANs used internally by the device (defined by the user).

Syntax

show vlan internal usage

Parameters
N/A

Default Configuration
N/A

Command Mode
Privileged EXEC mode

Example
The following example displays VLANs used internally by the device.

```
switchxxxxxx# show vlan internal usage

Usage          VLAN             Reserved       IP address
--------       --------         ----------     ----------
fe1/0/121      1007             No             Active
fe1/0/122      1008             Yes            Inactive
fe1/0/123      1009             Yes            Active
```

30.39 switchport access multicast-tv vlan

Use the **switchport access multicast-tv vlan** Interface Configuration (Ethernet, Port-channel) mode command to enable receiving Multicast transmissions on an interface that is not the access port VLAN, while keeping the L2 segregation with subscribers on different access port VLANs. Use the **no** form of this command to disable receiving Multicast transmissions.

Syntax
switchport access multicast-tv vlan *vlan-id*

no switchport access multicast-tv vlan

Parameters
vlan-id—Specifies the Multicast TV VLAN ID.

Default Configuration
Receiving Multicast transmissions is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
The user cannot transmit Multicast transmissions on the Multicast TV VLAN.

A Multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

Example
The following example enables `fe1/0/1`5 to receive Multicast transmissions from VLAN 11.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11
```

30.40 switchport customer multicast-tv vlan

Use the **switchport customer multicast-tv vlan** Interface Configuration mode command to enable receiving Multicast transmissions from a VLAN that is not the customer port's VLAN, while keeping the L2 segregation with subscribers on different customer port VLANs.

Syntax

switchport customer multicast-tv vlan *{**add** vlan-list* | ***remove** vlan-list}*

Parameters

- **add** *vlan-list*—Specifies a list of Multicast TV VLANs to add to interface.
- **remove** *vlan-list*—Specifies a list of Multicast TV VLANs to remove from interface.

Default Configuration

The port is not a member in any Multicast TV VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The user cannot transmit Multicast transmissions on Multicast TV VLANs.

A Multicast TV VLAN cannot be enabled if a Guest VLAN is enabled on the interface.

Example

The following example enables fe1/0/15 to receive Multicast transmissions from VLANs 5, 6, 7.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

30.41 show vlan multicast-tv

Use the **show vlan Multicast-tv** EXEC mode command to display the source and receiver ports of Multicast-TV VLAN. Source ports can transmit and receive traffic to/from the VLAN, while receiver ports can only receive traffic from the VLAN.

Syntax

show vlan Multicast-tv vlan *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID.

Default Configuration

N/A

Command Mode
EXEC mode

Example
The following example displays information on the source and receiver ports of Multicast-TV VLAN 1000.

```
switchxxxxxx# show vlan multicast-tv vlan 1000

Source Ports    Receiver Ports
------------    ----------------------
fe1/0/18,       fe1/0/11-18
fe1/0/19
```

31 Internet Group Management Protocol (IGMP) Snooping Commands

31.1 ip igmp snooping (Global)

Use the **ip igmp snooping** Global Configuration mode command to enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable IGMP snooping.

Syntax

ip igmp snooping

no ip igmp snooping

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables IGMP snooping.

```
switchxxxxxx(config)# ip igmp snooping
```

31.2 ip igmp snooping vlan

Use the **ip igmp snooping vlan** Global Configuration mode command to enable IGMP snooping on a specific VLAN. Use the **no** form of this command to disable IGMP snooping on a VLAN interface.

Syntax

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Parameters

vlan *vlan-id*—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2 and IGMPv3 are supported.

To activate IGMP snooping, the bridge multicast filtering should be enabled.

The user guidelines of the bridge multicast mode Interface VLAN Configuration command describes the configuration that is written into the FDB as a function of the FDB mode and the IGMP version that is used in the network.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

31.3 ip igmp snooping vlan mrouter

Use the **ip igmp snooping mrouter** Global Configuration mode command to enable automatic learning of Multicast router ports on a VLAN. Use the **no** form of this command to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

no ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

Parameters

vlan *vlan-id*—Specifies the VLAN.

Default Configuration

Learning pim-dvmrp is enabled.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports are learned according to:

- Queries received on the port
- PIM/PIMv2 received on the port
- DVMRP received on the port
- MRDISC received on the port
- MOSPF received on the port

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

31.4 ip igmp snooping vlan mrouter interface

Use the **ip igmp snooping mrouter interface** Global Configuration mode command to define a port that is connected to a Multicast router port. Use the **no** form of this command to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter interface** i*nterface-list*

no ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-list*

Parameters

- **vlan** *vlan-id*—Specifies the VLAN.
- **interface** *interface-list*—Specifies the list of interfaces. The interfaces can be one of the following types: Ethernet port or Port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

A port that is defined as a Multicast router port receives all IGMP packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 mrouter interface fe1/0/11
```

31.5 ip igmp snooping vlan forbidden mrouter interface

Use the **ip igmp snooping forbidden mrouter interface** Global Configuration mode command to forbid a port from being defined as a Multicast router port by static configuration or by automatic learning. Use the **no** form of this command to remove the configuration.

Syntax

ip igmp snooping vlan *vlan-id* **forbidden mrouter interface** *interface-list*

no ip igmp snooping **vlan** vlan-id **forbidden** mrouter **interface** interface-list

Parameters

- **vlan** *vlan-id*—Specifies the VLAN.
- **interface** *interface-list*—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration
No ports defined.

Command Mode
Global Configuration mode

User Guidelines
A port that is a forbidden mrouter port cannot be a Multicast router port (i.e. cannot be learned dynamically or assigned statically).

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 forbidden mrouter
interface fe1/0/11
```

31.6 ip igmp snooping vlan static
Use the **ip igmp snooping vlan static** Global Configuration mode command to register an IP-layer Multicast address to the bridge table, and to add static ports to the group defined by this address. Use the **no** form of this command to remove ports specified as members of a static Multicast group.

Syntax
ip igmp snooping vlan *vlan-id* **static** *ip-address [***interface** *interface-list]*

no ip igmp snooping vlan *vlan-id* **static** *ip-address [***interface** *interface-list]*

Parameter
- **vlan** *vlan-id*—Specifies the VLAN.
- **static** *ip-address*—Specifies the IP Multicast address.
- **interface** i*nterface-list*—Specifies a list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration
No Multicast addresses are defined.

Command Mode
Global Configuration mode

User Guidelines
Static Multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no** command without a port-list removes the entry.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 static 239.2.2.2 interface
fe1/0/11
```

31.7 ip igmp snooping vlan multicast-tv

Use the **ip igmp snooping vlan multicast-tv** Global Configuration mode command to define the Multicast IP addresses that are associated with a Multicast TV VLAN. Use the **no** form of this command to remove all associations.

Syntax

ip igmp snooping vlan *vlan-id* **multicast-tv** *ip-multicast-address [***count** *number]*

no ip igmp snooping vlan *vlan-id* **multicast-tv** *ip-multicast-address [***count** *number]*

Parameters

- **vlan-id**—Specifies the VLAN
- **count** *number*—Configures multiple contiguous Multicast IP addresses. If not specified, the default is 1. (Range: 1–256)

Default Configuration

No Multicast IP address is associated.

Command Mode

Global Configuration mode

User Guidelines

Use this command to define the Multicast transmissions on a Multicast-TV VLAN. The configuration is only relevant for an Access port that is a member in the configured VLAN as a Multicast-TV VLAN.

If an IGMP message is received on such an Access port, it is associated with the Multicast-TV VLAN only if it is for one of the Multicast IP addresses that are associated with the Multicast-TV VLAN.

Up to 256 VLANs can be configured.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 multicast-tv 239.2.2.2
count 3
```

31.8 ip igmp snooping map cpe vlan

The **ip igmp snooping map cpe vlan** Global Configuration mode command maps CPE VLANs to Multicast-TV VLANs. Use the **no** form of this command to remove the mapping.

Syntax

ip igmp snooping map cpe vlan *vlan-id multicast-tv* **vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

Parameters

- **cpe vlan** vlan-id—Specifies the CPE VLAN ID.

- **multicast-tv vlan** vlan-id—Specifies the Multicast-TV VLAN ID.

Default Configuration
No mapping exists.

Command Mode
Global Configuration mode

User Guidelines
Use this command to associate the CPE VLAN with a Multicast-TV VLAN.

If an IGMP message is received on a customer port tagged with a CPE VLAN, and there is mapping from that CPE VLAN to a Multicast-TV VLAN, the IGMP message is associated with the Multicast-TV VLAN.

Example
The following example maps CPE VLAN 2 to Multicast-TV VLAN 31.

```
switchxxxxxx(config)# ip igmp snooping map cpe vlan 2 multicast-tv vlan
31
```

31.9 ip igmp snooping vlan querier
Use the **ip igmp snooping vlan querier** Global Configuration mode command to enable the Internet Group Management Protocol (IGMP) querier on a specific VLAN. Use the **no** form of this command to disable the IGMP querier on a VLAN interface.

Syntax
ip igmp snooping vlan *vlan-id* **querier**

no ip igmp snooping vlan *vlan-id* **querier**

Parameters
vlan *vlan-id*—Specifies the VLAN

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
The IGMP snooping querier can be enabled on a VLAN only if IGMP snooping is enabled for that VLAN.

At most one switch can be configured as an IGMP Querier for a VLAN.

When the IGMP snooping querier is enabled, it starts after a host-time-out/2 with no IGMP traffic being detected from a Multicast router.

The IGMP Snooping Querier disables itself if it detects IGMP traffic from a Multicast router. It restarts automatically after host-time-out/2.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```

31.10 ip igmp snooping vlan querier address

Use the **ip igmp snooping vlan querier address** Global Configuration mode command to define the source IP address that the IGMP snooping querier uses. Use the **no** form of this command to return to default.

Syntax

ip igmp snooping vlan *vlan-id* **querier address** *ip-address*

no ip igmp snooping vlan *vlan-id* **querier address**

Parameters

- **vlan** *vlan-id*—Specifies the VLAN.
- **querier address** *ip-address*—Source IP address.

Default Configuration

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If there are multiple IP addresses, the minimum IP address defined on the VLAN is used.

Command Mode

Global Configuration mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the querier's VLAN, the querier is disabled.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier address
10.5.234.205
```

31.11 ip igmp snooping vlan querier version

Use the **ip igmp snooping vlan querier version** Global Configuration mode command to configure the IGMP version of an IGMP querier on a specific VLAN. Use the **no** form of this command to return to the default version.

Syntax

ip igmp snooping vlan *vlan-id* **querier version** *{2 | 3}*

no ip igmp snooping vlan *vlan-id* **querier version**

Parameters

- **vlan** *vlan-id*—Specifies the VLAN.
- **querier version** *2*—Specifies that the IGMP version would be IGMPv2.

- **querier version** *3*—Specifies that the IGMP version would be IGMPv3.

Default Configuration
IGMPv2.

Command Mode
Global Configuration mode

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

31.12 ip igmp robustness

Use the **ip igmp robustness** Interface Configuration (VLAN) mode command to set the IGMP robustness variable on a VLAN. Use the **no** format of the command to return to default.

Syntax
ip igmp robustness *count*

no ip igmp robustness

Parameters
count—The number of expected packet loss on a link. Parameter range. (Range: 1–7)

Default Configuration
2

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created, but you must enter the command in Interface VLAN mode.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp robustness 3
```

31.13 ip igmp query-interval

Use the **ip igmp query-interval** Interface Configuration (VLAN) mode command to configure the Query interval on a VLAN. Use the **no** format of the command to return to default.

Syntax
ip igmp query-interval *seconds*

no ip igmp query-interval

Parameters
seconds—Frequency, in seconds, at which IGMP query messages are sent on the interface. (Range: 30–18000)

Default Configuration
125

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp query-interval 200
```

31.14 ip igmp query-max-response-time
Use the **ip igmp query-max-response-time** Interface Configuration (VLAN) mode command to configure the Query Maximum Response time on a VLAN. Use the **no** format of the command to return to default.

Syntax
ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Parameters
seconds—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

Default Configuration
10

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp query-max-response-time 20
```

31.15 ip igmp last-member-query-count

Use the **ip igmp last-member-query-count** Interface Configuration (VLAN) mode command to configure the Last Member Query Counter on a VLAN. Use the **no** format of the command to return to default.

Syntax

ip igmp last-member-query-count *count*

no ip igmp last-member-query-count

Parameter

count—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of Robustness variable

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-count 7
```

31.16 ip igmp last-member-query-interval

Use the **ip igmp last-member-query-interval** Interface Configuration (VLAN) mode command to configure the Last Member Query interval on a VLAN. Use the **no** format of the command to return to default.

Syntax

ip igmp last-member-query-interval *milliseconds*

no ip igmp last-member-query-interval

Parameters

milliseconds—Interval, in milliseconds, at which IGMP group-specific host query messages are sent on the interface. (Range: 100–25500)

Default Configuration

1000

Command Mode

Interface Configuration (VLAN) mode

User Guidelines
You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-interval 2000
```

31.17 ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping vlan immediate-leave** Global Configuration mode command to enable the IGMP Snooping Immediate-Leave processing on a VLAN. Use the **no** format of the command to disable IGMP Snooping Immediate-Leave processing.

Syntax
ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Parameters
vlan *vlan-id*—Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration
Disabled

Command Mode
Global Configuration mode

User Guidelines
You can execute the command before the VLAN is created.

Example
The following example enables IGMP snooping immediate-leave feature on VLAN 1.

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

31.18 show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** EXEC mode command displays information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN.

Syntax
show ip igmp snooping mrouter *[***interface** *vlan-id*]

Parameters
interface *vlan-id*—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000.

```
switchxxxxxx# show ip igmp snooping mrouter interface
1000


VLAN       Dynamic       Static      Forbidden
----       ------        -------     ---------
1000       fe1/0/11      fe1/0/12    fe1/0/13-23
```

31.19 show ip igmp snooping interface
The **show ip igmp snooping interface** EXEC mode command displays the IGMP snooping configuration for a specific VLAN.

Syntax
show ip igmp snooping interface *vlan-id*

Parameters
interface vlan-id—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays the IGMP snooping configuration for VLAN 1000

```
switchxxxxxx# show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping admin: Enabled
IGMP Snooping oper: Enabled
Routers IGMP version: 3
Groups that are in IGMP version 2 compatibility mode:
231.2.2.3, 231.2.2.3
Groups that are in IGMP version 1 compatibility mode:
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3
IGMP snooping robustness: admin 2  oper 2
IGMP snooping query interval: admin 125 sec oper 125 sec
```

```
IGMP snooping query maximum response: admin 10 sec oper 10 sec
IGMP snooping last member query counter: admin 2 oper 2
IGMP snooping last member query interval: admin 1000 msec oper 500 msec
IGMP snooping last immediate leave: enable
Automatic learning of Multicast router ports is enabled
```

31.20 show ip igmp snooping groups

The **show ip igmp snooping groups** EXEC mode command displays the Multicast groups learned by the IGMP snooping.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [*address ip-multicast-address*] [*source ip-address*]

Parameters

vlan *vlan-id*—Specifies the VLAN ID.

address ip-multicast-address—Specifies the IP multicast address.

source ip-address—Specifies the IP source address.

Command Mode

EXEC mode

User Guidelines

To see all Multicast groups learned by IGMP snooping, use the **show ip igmp snooping groups** command without parameters.

Use the **show ip igmp snooping groups** command with parameters to see a needed subset of all Multicast groups learned by IGMP snooping

To see the full Multicast address table (including static addresses), use the **show bridge multicast address-table** command.

Example

The following example shows sample output for IGMP version 2.

```
switchxxxxxx# show ip igmp snooping groups

Vlan    Group             Source       Include Ports       Exclude Ports      Comp-Mode
        Address           Address
----    ---------         --------     ---------           --------           ---------
1       239.255.255.250   *            gi1                                    v3
```

31.21 show ip igmp snooping multicast-tv

The **show ip igmp snooping multicast-tv** EXEC mode command displays the IP addresses associated with Multicast TV VLANs.

Syntax

show ip igmp snooping multicast-tv *[***vlan** *vlan-id*]

Parameters
vlan *vlan-id*—Specifies the VLAN ID.

Command Mode
EXEC mode

Example
The following example displays the IP addresses associated with all Multicast TV VLANs.

```
switchxxxxxx# show ip igmp snooping multicast-tv
VLAN IP Address
---- -----------
1000 239.255.0.0
1000 239.255.0.1
1000 239.255.0.2
1000 239.255.0.3
1000 239.255.0.4
1000 239.255.0.5
1000 239.255.0.6
1000 239.255.0.7
```

31.22 show ip igmp snooping cpe vlans
The **show ip igmp snooping cpe vlans** EXEC mode command displays the CPE VLAN to Multicast TV VLAN mappings.

Syntax
show ip igmp snooping cpe vlans *[***vlan** *vlan-id*]

Parameters
vlan *vlan-id* —Specifies the CPE VLAN ID.

Command Mode
EXEC mode

Example
The following example displays the CPE VLAN to Multicast TV VLAN mappings.

```
switchxxxxxx# show ip igmp snooping cpe vlans
CPE VLAN  Multicast-TV VLAN
--------  ------------------
2         1118
3         1119
```

32 IPv6 MLD Snooping Commands

32.1 ipv6 mld snooping (Global)

The **ipv6 mld snooping** Global Configuration mode command enables IPv6 Multicast Listener Discovery (MLD) snooping. To disable IPv6 MLD snooping, use the **no** form of this command.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Parameters

N/A

Default Configuration

IPv6 MLD snooping is disabled.

Command Mode

Global Configuration mode

Example

The following example enables IPv6 MLD snooping.

```
switchxxxxxx(config)# ipv6 mld snooping
```

32.2 ipv6 mld snooping vlan

Use the **ipv6 mld snooping vlan** Global Configuration mode command to enable MLD snooping on a specific VLAN. Use the **no** form of this command to disable MLD snooping on a VLAN interface.

Syntax

ipv6 mld snooping vlan *vlan-id*

no ipv6 mld snooping vlan *vlan-id*

Parameters

vlan-id—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

MLD snooping can only be enabled on static VLANs.

MLDv1 and MLDv2 are supported.

To activate MLD snooping, the Bridge Multicast Filtering command must be enabled.

The user guidelines of the bridge multicast ipv6 mode Interface VLAN Configuration command describe the configuration that can be written into the FDB as a function of the FDB mode, and the MLD version that is used in the network.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 2
```

32.3 ipv6 mld robustness

Use the **ipv6 mld robustness i**nterface Configuration mode command to change a value of MLD robustness. Use the **no** format of the command to return to default.

Syntax

ipv6 mld robustness *count*

no ipv6 mld robustness

Parameters

count - The number of expected packet losses on a link. (Range: 1–7)

Default Configuration

2

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld robustness 3
```

32.4 ipv6 mld snooping mrouter

Use the **ipv6 mld snooping mrouter** Global Configuration mode command to enable automatic learning of Multicast router ports. Use the **no** form of this command to remove the configuration.

Syntax

ipv6 mld snooping vlan *vlan-id* **mrouter learn** ***pim-dvmrp***

no ipv6 mld snooping vlan *vlan-id* **mrouter learn** ***pim-dvmrp***

Parameters

- **vlan-id**—Specifies the VLAN.

- **pim-dvmrp**—Learn Multicast router port by PIM, DVMRP and MLD messages.

Default Configuration

Learning **pim-dvmrp** is enabled.

Command Mode

Global Configuration mode

User Guidelines

Multicast router ports can be configured statically with the bridge multicast forward-all command.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

32.5 ipv6 mld snooping mrouter interface

Use the **ipv6 mld snooping mrouter interface** Global Configuration mode command to define a port that is connected to a Multicast router port. Use the **no** form of this command to remove the configuration.

Syntax

ipv6 mld snooping *vlan* *vlan-id* **mrouter interface** *interface-list*

no ipv6 mld snooping *vlan* *vlan-id* **mrouter interface** *interface-list*

Parameters

- **vlan-id**—Specifies the VLAN.
- **interface-list**—Specifies a list of interfaces. The interfaces can be from one of the following types: port or port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

This command may be used in conjunction with the bridge multicast forward-all command, which is used in older versions to statically configure a port as a Multicast router.

A port that is defined as a Multicast router port receives all MLD packets (reports and queries) as well as all Multicast data.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter interface
fe1/0/11
```

32.6 ipv6 mld snooping forbidden mrouter interface

Use the **ipv6 mld snooping forbidden mrouter interface** Global Configuration mode command to forbid a port from being defined as a Multicast router port by static configuration or by automatic learning. Use the **no** form of this command to remove the configuration.

Syntax

ipv6 mld snooping *vlan* *vlan-id* **forbidden mrouter *interface*** *interface-list*

no ipv6 mld snooping *vlan* *vlan-id* **forbidden mrouter *interface*** *interface-list*

Parameters

- **vlan-id**—Specifies the VLAN.
- **interface-list**—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No forbidden ports by default

Command Mode

Global Configuration mode

User Guidelines

A port that is forbidden to be defined as a Multicast router port (mrouter port) cannot be learned dynamically or assigned statically.

The bridge multicast forbidden forward-all command was used in older versions to forbid dynamic learning of Multicast router ports.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter
interface fe1/0/11
```

32.7 ipv6 mld snooping static

Use the **ipv6 mld snooping static** Global Configuration mode command to register a IPv6-layer Multicast address to the bridge table, and to add statically ports to the group. Use the **no** form of this command to remove ports specified as members of a static Multicast group.

Syntax

ipv6 mld snooping *vlan* *vlan-id* **static** *ipv6-address* ***interface*** *[interface-list]*

no ipv6 mld snooping *vlan* *vlan-id* **static** *ipv6-address* ***interface*** *[interface-list]*

Parameters

- **vlan-id**—Specifies the VLAN.
- **ipv6-address**—Specifies the IP multicast address

- **interface-list**—Specifies list of interfaces. The interfaces can be from one of the following types: Ethernet port or Port-channel.

Default Configuration

No Multicast addresses are defined.

Command Mode

Global configuration mode

User Guidelines

Static multicast addresses can only be defined on static VLANs.

You can execute the command before the VLAN is created.

You can register an entry without specifying an interface.

Using the **no** command without a port-list removes the entry.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 static 239.2.2.2 fe1/0/11
```

32.8 ipv6 mld query-interval

Use the **ipv6 mld query-interval** Interface Configuration mode command to configure the Query interval. Use the **no** format of the command to return to default.

Syntax

ipv6 mld query-interval *seconds*

ipv6 mld query-interval

Parameters

seconds—Frequency, in seconds, at which MLD query messages are sent on the interface. (Range: 30–18000)

Default Configuration

125

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides the frequency value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld query-interval 3000
```

32.9 ipv6 mld query-max-response-time

Use the **ipv6 mld query-max-response-time** Interface Configuration mode command to configure the Query Maximum Response time. Use the **no** format of the command to return to default.

Syntax

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

Parameter

seconds—Maximum response time, in seconds, advertised in MLD queries. (Range: 5–20)

Default Configuration

10

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

This command provides the maximum response time value if this value is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

switchxxxxxx(config)# **interface vlan** 1

switchxxxxxx(config-if)# **ipv6 mld query-max-response-time** 5

32.10 ipv6 mld last-member-query-count

Use the **ipv6 mld last-member-query-count** Interface Configuration mode command to configure the Last Member Query Count. This is the number of Multicast address specific queries sent before the router assumes there are no local listeners.The Last Listener Query Count is also the number of Multicast Address and Source Specific Queries sent before the router assumes there are no listeners for a particular source.

Use the **no** format of the command to return to default.

Syntax

ipv6 mld last-member-query-count *count*

no ipv6 mld last-member-query-count

Parameters

count—The number of times that group- or group-source-specific queries are sent upon receipt of a Leave message. (Range: 1–7)

Default Configuration

The value of the Robustness variable.

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
This command provides this value if it is not is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld last-member-query-count 3
```

32.11 ipv6 mld last-member-query-interval
Use the **ipv6 mld last-member-query-interval** interface configuration command to configure the Last Member Query Interval. Use the **no** format of the command to return to default.

Syntax
ipv6 mld last-member-query-interval *milliseconds*

no ipv6 mld last-member-query-interval

Parameter
milliseconds—Interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. (Range: 100–64512).

Default Configuration
1000

Command Mode
Interface Configuration (VLAN) mode

User Guidelines
This command provides this value if it is not is not received in MLD general query messages. A field for this value is present in MLDv2 general query messages, but this field may be blank. There is no field for this value in MLDv1 general query messages.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld last-member-query-interval 2000
```

32.12 ipv6 mld snooping vlan immediate-leave
Use the **ipv6 mld snooping vlan immediate-leave** Global Configuration mode command to enable MLD Snooping Immediate-Leave processing on a VLAN. When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD

queries from the Multicast router, it deletes entries periodically if it does not receive any MLD membership reports from the Multicast clients.

MLD snooping Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface.

Use the **no** format of the command to return to disable MLD Snooping Immediate-Leave processing.

Syntax

ipv6 mld snooping vlan *vlan-id* **immediate-leave**

no ipv6 mld snooping vlan *vlan-id* **immediate-leave**

Parameters

vlan-id—Specifies the VLAN ID value. (Range: 1–4094)

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 immediate-leave
```

32.13 show ipv6 mld snooping mrouter

The **show ipv6 mld snooping mrouter** EXEC mode command displays information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN.

Syntax

show ipv6 mld snooping mrouter ***[interface*** *vlan-id*]

Parameters

interface vlan-id—Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode

EXEC mode

Example

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000

```
switchxxxxxx# show ipv6 mld snooping mrouter interface 1000
VLAN   Static    Dynamic   Forbidden
----   ------    -------   ---------
1000   fe1/0/11  fe1/0/12       fe1/0/13-23
```

32.14 show ipv6 mld snooping interface

The **show ipv6 mld snooping interface** EXEC mode command displays the IPv6 MLD snooping configuration for a specific VLAN.

Syntax

show ipv6 mld snooping interface *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode

EXEC mode

Example

The following example displays the MLD snooping configuration for VLAN 1000.

```
switchxxxxxx# show ipv6 mld snooping interface 1000
MLD Snooping is globally enabled
MLD Snooping admin: Enabled
MLD snooping oper mode: Enabled
Routers MLD version: 2
Groups that are in MLD version 1 compatibility mode:
FF12::3, FF12::8
MLD snooping robustness:admin 2  oper 2
MLD snooping query interval: admin 125 sec  oper 125 sec
MLD snooping query maximum response: admin 10 sec  oper 10 sec
MLD snooping last member query counter: admin 2  oper 2
MLD snooping last member query interval: admin 1000 msec  oper 600 msec
MLD snooping last immediate leave: enable
Automatic learning of multicast router ports is enabled
```

32.15 show ipv6 mld snooping groups

The **show ipv6 mld snooping groups** EXEC mode command displays the multicast groups learned by the MLD snooping.

Syntax

show ipv6 mld snooping groups *[**vlan** vlan-id*] *[**address** ipv6-multicast-address] [**source** ipv6-address]*

Parameters

- **vlan vlan-id**—Specifies the VLAN ID.
- **address ipv6-multicast-address**—Specifies the IPv6 multicast address.
- **source ipv6-address**—Specifies the IPv6 source address.

Command Mode

EXEC mode

Default Configuration

Display information for all VLANs and addresses defined on them.

User Guidelines

To see the full multicast address table (including static addresses), use the **show bridge multicast address-table** command.

The Include list contains the ports which are in a forwarding state for this group according to the snooping database. In general, the Exclude list contains the ports which have issued an explicit Exclude for that specific source in a multicast group.

The Reporters That Are Forbidden Statically list contains the list of ports which have asked to receive a multicast flow but were defined as forbidden for that multicast group in a multicast bridge.

Note: Under certain circumstances, the Exclude list may not contain accurate information; for example, in the case when two Exclude reports were received on the same port for the same group but for different sources, the port will not be in the Exclude list but rather in the Include list

Example

The following example shows the output for IPv6 MLD version 2.

```
switchxxxxxx# show ipv6 mld snooping groups

VLAN    Group Address   Source Address            Include Ports   Exclude Ports   Compatibility Mode
----    --------        -----------------------  -------------   -------------   ------------------
1       FF12::3         FE80::201:C9FF:FE40:8001 fe1/0/11        ------------    1
1       FF12::3         FE80::201:C9FF:FE40:8002 fe1/0/12                        1
19      FF12::8         FE80::201:C9FF:FE40:8003 fe1/0/19                        2
19      FF12::8         FE80::201:C9FF:FE40:8004 fe1/0/11                        2
19      FF12::8         FE80::201:C9FF:FE40:8005 fe1/0/110-11    fe1/0/12        2
                                                                 fe1/0/13
```

```
MLD Reporters that are forbidden statically:
VLAN    Group Address   Source Address              Ports
----    -------------   ------------------------   --------
1       FF12::3         FE80::201:C9FF:FE40:8001   fe1/0/18
19      FF12::8         FE80::201:C9FF:FE40:8001   fe1/0/19
```

33 Link Aggregation Control Protocol (LACP) Commands

33.1 lacp system-priority

Use the **lacp system-priority** Global Configuration mode command to set the system priority. Use the **no** form of this command to restore the default configuration.

Syntax

lacp system-priority *value*

no lacp system-priority

Parameters

value—Specifies the system priority value. (Range: 1–65535)

Default Configuration

The default system priority is 1.

Command Mode

Global Configuration mode

Example

The following example sets the system priority to 120.

```
switchxxxxxx(config)# lacp system-priority 120
```

33.2 lacp port-priority

Use the **lacp port-priority** Interface Configuration (Ethernet) mode command to set the physical port priority. Use the **no** form of this command to restore the default configuration.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

value—Specifies the port priority. (Range: 1use the **no** form of this command65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface Configuration (Ethernet) mode

Example
The following example sets the priority of fe1/0/16.

```
switchxxxxxx(config)# interface fe1/0/16
switchxxxxxx(config-if)# lacp port-priority 247
```

33.3 lacp timeout
Use the **lacp timeout** Interface Configuration (Ethernet) mode command to assign an administrative LACP timeout to an interface. Use the **no** form of this command to restore the default configuration.

Syntax
lacp timeout ***{long*** | ***short}***

no lacp timeout

Parameters
- **long**—Specifies the long timeout value.
- **short**—Specifies the short timeout value.

Default Configuration
The default port timeout value is Long.

Command Mode
Interface Configuration (Ethernet) mode

Example
The following example assigns a long administrative LACP timeout to fe1/0/16.

```
switchxxxxxx(config)# interface fe1/0/16
switchxxxxxx(config-if)# lacp timeout long
```

33.4 show lacp
Use the **show lacp** EXEC mode command to display LACP information for all Ethernet ports or for a specific Ethernet port.

Syntax
show lacp *interface-id [**parameters*** | ***statistics*** | ***protocol-state***]

Parameters
- **interface-id** —Specify an interface ID. The interface ID must be an Ethernet port
- **parameters**—Displays parameters only.
- **statistics**—Displays statistics only.
- **protocol-state**—Displays protocol state only.

Command Mode
EXEC mode

Example
The following example displays LACP information for fe1/0/11.

```
switchxxxxxx# show lacp ethernet fe1/0/11

Port fe1/0/11 LACP parameters:

     Actor

            system priority:            1
            system mac addr:            00:00:12:34:56:78
            port Admin key:             30
            port Oper key:              30
            port Oper number:           21
            port Admin priority:        1
            port Oper priority:         1
            port Admin timeout:         LONG
            port Oper timeout:          LONG
            LACP Activity:              ACTIVE
            Aggregation:                AGGREGATABLE
            synchronization:            FALSE
            collecting:                 FALSE
            distributing:               FALSE
            expired:                    FALSE

     Partner

            system priority:            0
            system mac addr:            00:00:00:00:00:00
            port Admin key:             0
            port Oper key:              0
            port Oper number:           0
            port Admin priority:        0
            port Oper priority:         0
            port Admin timeout:         LONG
            port Oper timeout:          LONG
            LACP Activity:              PASSIVE
            Aggregation:                AGGREGATABLE
            synchronization:            FALSE
            collecting:                 FALSE
            distributing:               FALSE
            expired:                    FALSE

Port fe1/0/11 LACP Statistics:
LACP PDUs sent:                         2
LACP PDUs received:                     2

Port fe1/0/11 LACP Protocol State:

     LACP State Machines:

            Receive FSM:                Port Disabled State
            Mux FSM:                    Detached State

     Control Variables:
```

```
        BEGIN:                      FALSE
        LACP_Enabled:               TRUE
        Ready_N:                    FALSE
        Selected:                   UNSELECTED
        Port_moved:                 FALSE
        NNT:                        FALSE
        Port_enabled:               FALSE

    Timer counters:

        periodic tx timer:          0
        current while timer:        0
        wait while timer:           0
```

33.5 show lacp port-channel

Use the **show lacp port-channel** EXEC mode command to display LACP information for a port-channel.

Syntax

show lacp port-channel *[port_channel_number]*

Parameters

port_channel_number—Specifies the port-channel number.

Command Mode

EXEC mode

Example

The following example displays LACP information about port-channel 1.

```
switchxxxxxx# show lacp port-channel 1


Port-Channel 1:Port Type 1000 Ethernet

      Actor

                System              1
                Priority:           000285:0E1C00
                MAC Address:        29
                Admin Key:          29
                Oper Key:


      Partner

                System              0
                Priority:           00:00:00:00:00:00
                MAC Address:        14
                Oper Key:
```

34 GARP VLAN Registration Protocol (GVRP) Commands

34.1 gvrp enable (Global)

Use the **gvrp enable** Global Configuration mode command to enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally. Use the **no** form of this command to disable GVRP on the device.

Syntax

gvrp enable

no gvrp enable

Parameters

N/A

Default Configuration

GVRP is globally disabled.

Command Mode

Global Configuration mode

Example

The following example enables GVRP globally on the device.

```
switchxxxxxx(config)# gvrp enable
```

34.2 gvrp enable (Interface)

Use the **gvrp enable** Interface Configuration (Ethernet, Port-channel) mode command to enable GVRP on an interface. Use the **no** form of this command to disable GVRP on an interface.

Syntax

gvrp enable

no gvrp enable

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

An access port does not dynamically join a VLAN because it is always a member of a single VLAN only. Membership in an untagged VLAN is propagated in the same way as in a tagged VLAN. That is, the PVID must be manually defined as the untagged VLAN ID.

Example

The following example enables GVRP on `fe1/0/16`.

```
switchxxxxxx(config)# interface fe1/0/16
switchxxxxxx(config-if)# gvrp enable
```

34.3 garp timer

Use the **garp timer** Interface Configuration mode command to adjust the values of the join, leave and leaveall timers of GARP applications, such as GVRP. Use the **no** form of this command to restore the default configuration.

Syntax

garp timer ***{join*** | ***leave*** | ***leaveall}*** ***timer-value***

no garp timer

Parameters

- The following specify the type of timer. The possible values are:
  - **join**—Specifies the GARP join timer. The timer value for this type of timer specifies the time interval between the two join messages sent by the GARP application.
  - **leave**—Specifies the GARP leave timer. The timer value for this type of timer specifies the time interval for a GARP application to wait for a join message after receiving a leave message for a GARP attribute, before it de-registers the GARP attribute.
  - **leaveall**—Specifies the GARP leaveall timer. The timer value for this type of timer specifies the time interval between leaveall messages for a GARP entity, which prompt other GARP entities to re-reregister all attribute information on this entity.
- **timer-value**—Specifies the timer value in milliseconds in multiples of 10. (Range: 10–2147483640)

Default Configuration

The following are the default timer values:

- **Join timer**—200 milliseconds
- **Leave timer**—600 milliseconds
- **Leaveall timer**—10000 milliseconds

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The **timer-value** must be a multiple of 10.

The following relationship must be maintained between the timers:

- The leave timer value must be greater than or equal to three times the join timer.

- The leave-all timer value must be greater than the leave timer.

Set the same GARP timer values on all Layer 2-connected devices to ensure proper operation of the GARP application.

Example

The following example sets the leave timer for `fe1/0/16` to 900 milliseconds.

```
switchxxxxxx(config)# interface fe1/0/16
switchxxxxxx(config-if)# garp timer leave 900
```

34.4 gvrp vlan-creation-forbid

Use the **gvrp vlan-creation-forbid** Interface Configuration mode command to disable dynamic VLAN creation or modification. Use the **no** form of this command to enable dynamic VLAN creation or modification.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Default Configuration

Enabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example disables dynamic VLAN creation on `fe1/0/13`.

```
switchxxxxxx(config)# interface fe1/0/13
switchxxxxxx(config-if)# gvrp vlan-creation-forbid
```

34.5 gvrp registration-forbid

Use the **gvrp registration-forbid** Interface Configuration mode command to deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port. Use the **no** form of this command to allow dynamic registration of VLANs on a port.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example forbids dynamic registration of VLANs on fe1/0/12.

```
switchxxxxxx(config)# interface fe1/0/12
switchxxxxxx(config-if)# gvrp registration-forbid
```

34.6 clear gvrp statistics
Use the **clear gvrp statistics** Privileged EXEC mode command to clear GVRP statistical information for all interfaces or for a specific interface.

Syntax
clear gvrp statistics *[interface-id]*

Parameters
Interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
All GVRP statistics are cleared.

Command Mode
Privileged EXEC mode

Example
The following example clears all GVRP statistical information on fe1/0/15.

```
switchxxxxxx# clear gvrp statistics fe1/0/15
```

34.7 show gvrp configuration
Use the **show gvrp configuration** EXEC mode command to display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP.

Syntax
show gvrp configuration *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
All GVRP statistics are displayed.

Command Mode
EXEC mode

Example
The following example displays GVRP configuration.

```
switchxxxxxx# show gvrp configuration
GVRP Feature is currently Enabled on the device.
Maximum VLANs: 4094
Port GVRP-Status Regist-    Dynamic          Timers(ms)
                 ration     VLAN Creation    Leave   Join   Leave All
---- ----------- --------   -------------    ----    -----  ----
fe1/0/11   Enabled     Forbidden Disabled         200     600    10000
fe1/0/12   Enabled     Normal    Enabled          400     1200   20000
```

34.8 show gvrp statistics
Use the **show gvrp statistics** EXEC mode command to display GVRP statistics for all interfaces or for a specific interface.

Syntax
show gvrp statistics *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
All GVRP statistics are displayed.

Command Mode
EXEC mode

Example
The following example displays GVRP statistical information.

```
switchxxxxxx# show gvrp statistics
GVRP statistics:
----------------
Legend:
rJE :    Join Empty Received       rJIn: Join In Received
rEmp:    Empty Received            rLIn: Leave In Received
rLE :    Leave Empty Received      rLA : Leave All Received
sJE :    Join Empty Sent           sJIn: Join In Sent
sEmp:    Empty Sent                sLIn: Leave In Sent
sLE :    Leave Empty Sent          sLA : Leave All Sent
```

```
Port     rJE   rJIn   rEmp   rLIn   rLE    rLA    sJE    sJIn   sEmp   sLIn   sLE    sLA
-----    ----  ----   ----   ----   ----   ----   ----   ----   ----   ----   ----   ---
fe1/0/11 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/12 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/13 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/14 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/15 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/16 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/17 0     0      0      0      0      0      0      0      0      0      0      0
fe1/0/18 0     0      0      0      0      0      0      0      0      0      0      0
```

34.9 show gvrp error-statistics

Use the **show gvrp error-statistics** EXEC mode command to display GVRP error statistics for all interfaces or for a specific interface.

Syntax

show gvrp error-statistics *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration

All GVRP error statistics are displayed.

Command Mode

EXEC mode

Example

The following example displays GVRP error statistics.

```
switchxxxxxx# show gvrp error-statistics
GVRP Error Statistics:
----------------------
Legend:
  INVPROT  : Invalid Protocol Id
  INVATYP  : Invalid Attribute Type  INVALEN : Invalid Attribute Length
  INVAVAL  : Invalid Attribute Value INVEVENT: Invalid Event
  Port   INVPROT INVATYP INVAVAL INVALEN INVEVENT
-------- ------- ------- ------- ------- --------
 fe1/0/11       0       0       0       0       0
 fe1/0/12       0       0       0       0       0
 fe1/0/13       0       0       0       0       0
 fe1/0/14       0       0       0       0       0
 fe1/0/15       0       0       0       0       0
 fe1/0/16       0       0       0       0       0
```

```
fe1/0/17        0         0         0         0         0
fe1/0/18        0         0         0         0         0
```

35 Voice VLAN Commands

Use the **voice vlan id** Global Configuration mode command to statically configure the VLAN identifier of the voice VLAN. The **no** format of the command returns the voice VLAN to the default VLAN (1).

Syntax

voice vlan id *vlan-id*

no voice vlan id

Parameters

vlan id *vlan-id*—Specifies the voice VLAN (range 1-4094).

Default Configuration

VLAN ID 1.

Command Mode

Global Configuration mode

User Guidelines

If the Voice VLAN does not exist, it is created automatically. It will not be removed automatically by the **no** version of this command.

Example

The following example enables VLAN 104 as the voice VLAN on the device.

```
switchxxxxxx(config)# voice vlan id 35
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCP
will cause the switch to advertise the administrative voice VLAN as static
voice VLAN which has higher priority than voice VLAN learnt from external
sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:19:36 %VLAN-I-VoiceVlanCreated: Voice Vlan ID 104 was
created.
switchxxxxxx(config)#30-Apr-2011 00:19:51 %VLAN-I-ReceivedFromVSDP: Voice
VLAN updated by VSDP. Voice VLAN-ID 104, VPT 5, DSCP 46
```

35.1 voice vlan oui-table

Use the **voice vlan oui-table** Global Configuration mode command to configure the voice OUI table. Use the **no** form of this command to restore the default configuration.

Syntax

voice vlan oui-table *{**add** mac-address-prefix* | ***remove** mac-address-prefix}* [*text*]

no voice vlan oui-table

Parameters

- **add** *mac-address-prefix*—Adds the specified MAC address prefix to the voice VLAN OUI table (length: 3 bytes).
- **remove** *mac-address-prefix*—Removes the specified MAC prefix address from the voice VLAN OUI table (length: 3 bytes).
- **text**—Adds the specified text as a description of the specified MAC address to the voice VLAN OUI table (length: 1–32 characters).

Default Configuration

The default voice VLAN OUI table is:

OUI	Description
00:e0:bb	3COM Phone
00:03:6b	Cisco Phone
00:e0:75	Veritel Polycom Phone
00:d0:1e	Pingtel Phone
00:01:e3	Siemens AG Phone
00:60:b9	NEC/Philips Phone
00:0f:e2	Huawei-3COM Phone
00:09:6e	Avaya Phone

Command Mode

Global Configuration mode

User Guidelines

The classification of a packet from VoIP equipment/phones is based on the packet's OUI in the source MAC address. OUIs are globally assigned (administered) by the IEEE.

In MAC addresses, the first three bytes contain a manufacturer ID (Organizationally Unique Identifiers (OUI)) and the last three bytes contain a unique station ID.

Since the number of IP phone manufacturers that dominates the market is limited and well known, the known OUI values are configured by default and OUIs can be added/removed by the user when required.

Example

The following example adds an entry to the voice VLAN OUI table.

```
switchxxxxxx(config)# voice vlan oui-table add 00:AA:BB description
experimental
```

35.2 voice vlan cos mode

Use the **voice vlan cos mode** Interface Configuration mode command to select the OUI voice VLAN Class of Service (CoS) mode. Use the **no** form of this command to return to the default.

Syntax

voice vlan cos mode ***{src*** | ***all}***

no voice vlan cos mode

Parameters

- **src**—QoS attributes are applied to packets with OUIs in the source MAC address. See the User Guidelines of voice vlan oui-table.
- **all**—QoS attributes are applied to packets that are classified to the Voice VLAN.

Default Configuration

The default mode is **src**.

Command Mode

Global Configuration mode

Example

The following example applies QoS attributes to voice packets.

```
switchxxxxxx(config)# voice vlan cos mode all
```

35.3 voice vlan cos

Use the **voice vlan cos** Global Configuration mode command to set the OUI Voice VLAN Class of Service (CoS). Use the **no** form of this command to restore the default configuration.

Syntax

voice vlan ***cos*** *cos* ***[remark]***

no voice vlan cos

Parameters

- **cos** *cos*—Specifies the voice VLAN Class of Service value. (Range: 0–7)
- **remark**—Specifies that the L2 user priority is remarked with the CoS value.

Default Configuration

The default CoS value is 5.

The L2 user priority is not remarked by default.

Command Mode

Global Configuration mode

Example

The following example sets the OUI voice VLAN CoS to 7 and does not do remarking.

```
switchxxxxxx(config)# voice vlan cos 7
```

35.4 voice vlan aging-timeout

Use the **voice vlan aging-timeout** Global Configuration mode command to set the OUI Voice VLAN aging timeout interval. Use the **no** form of this command to restore the default configuration.

Syntax

voice vlan aging-timeout *minutes*

no voice vlan aging-timeout

Parameters

aging-timeout *minutes*—Specifies the voice VLAN aging timeout interval in minutes. (Range: 1–43200).

Default Configuration

1440 minutes

Command Mode

Global Configuration mode

Example

The following example sets the OUI Voice VLAN aging timeout interval to 12 hours.

```
switchxxxxxx(config)# voice vlan aging-timeout 720
```

35.5 voice vlan enable

Use the **voice vlan enable** Interface Configuration (Ethernet, Port-channel) mode command to enable OUI voice VLAN configuration on an interface. Use the **no** form of this command to disable OUI voice VLAN configuration on an interface.

Syntax

voice vlan enable

no voice vlan enable

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command is applicable only if the voice VLAN state is globally configured as OUI voice VLAN (using voice vlan state).

The port is added to the voice VLAN if a packet with a source MAC address OUI address (defined by voice vlan oui-table) is trapped on the port. Note: The packet VLAN ID does not have to be the voice VLAN, it can be any VLAN.

The port joins the voice VLAN as a tagged port.

If the time since the last MAC address with a source MAC address OUI address was received on the interface exceeds the timeout limit (configured by voice vlan aging-timeout), the interface is removed from the voice VLAN.

Example

The following example enables OUI voice VLAN configuration on `fe1/0/12`.

```
switchxxxxxx(config)# interface fe1/0/12
switchxxxxxx(config-if)# voice vlan enable
```

35.6 voice vlan secure

Use the **voice vlan secure** Interface Configuration (Ethernet, Port-channel) mode command to enable the secure mode for the OUI voice VLAN. Use the **no** form of this command to disable the secure mode (see User Guidelines for an explanation of secure mode).

Syntax

voice vlan secure

no voice vlan secure

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Secure mode specifies that packets that are classified to the voice VLAN with a source MAC address that is not a OUI address (defined by voice vlan oui-table) are discarded.

This command is relevant only to ports that were added to the voice VLAN automatically.

Example

The following example enables the secure mode for the OUI Voice VLAN on `fe1/0/18`.

```
switchxxxxxx(config)# interface fe1/0/18
switchxxxxxx(config-if)# voice vlan secure
```

35.7 show voice vlan

Use the **show voice vlan** EXEC mode command to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI.

Syntax

show voice vlan [type {*oui* | *auto*}] [*interface-id***]**

Parameters

- **type oui**—Common and OUI-voice-VLAN specific parameters are displayed.
- **type auto**—Common and Auto Voice VLAN-specific parameters are displayed.
- **interface-id**—Specifies an Ethernet port ID. Relevant only for the OUI type.

Default Configuration

If the **type** parameter is omitted the current Voice VLAN type is used.

If interface-id parameter is omitted then information about all interfaces is displayed.

Command Mode

EXEC mode

User Guidelines

Using this command without parameters displays the current voice VLAN type parameters and local and agreed voice VLAN settings.

Using this command with the **type** parameter displays the voice VLAN parameters relevant to the type selected. The the local and agreed voice VLAN settings are displayed only if this is the current voice VLAN state.

The interface-id parameter is relevant only for the OUI VLAN type.

Examples:

The following examples display the output of this command in various configurations.

Example 1—Displays the **auto** voice VLAN parameters (this is independent of the voice VLAN state actually enabled).

```
switch>show voice vlan type auto
switchxxxxxx#show voice vlan type auto
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
switchxxxxxx#
```

Example 2—Displays the current voice VLAN parameters when the voice VLAN state is auto-enabled.

```
switch>show voice vlan
Administrate Voice VLAN state is auto-enabled
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
```

```
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 16:48:13
switchxxxxxx#
```

Example 3—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered but voice VLAN has not been triggered.

```
switch>show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is disabled
VSDP Authentication is disabled
```

Example 4—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered and it has been triggered.

```
switchxxxxxx(config)#voice vlan state auto-triggered
switchxxxxxx(config)#voice vlan state auto-triggered
operational voice vlan state is auto
admin state is auto triggered
switchxxxxxx#show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
```

Example 5—Displays the current voice VLAN parameters when both auto voice VLAN and OUI are disabled.

```
switch>show voice vlan
switchxxxxxx#show voice vlan
Administrate Voice VLAN state is disabled
Operational Voice VLAN state is disabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Aging timeout: 1440 minutes
```

Example 5—Displays the voice VLAN parameters when the voice VLAN operational state is OUI.

```
switch>show voice vlan
Administrate Voice VLAN state is oui-enabled
Operational Voice VLAN state is oui-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 4
Best Local DSCP is 1
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes
OUI table
MAC Address - Prefix   Description
--------------------   ------------------
00:E0:BB               3COM
00:03:6B               Cisco
00:E0:75               Veritel
00:D0:1E               Pingtel
00:01:E3               Simens
00:60:B9               NEC/Philips
00:0F:E2               Huawei-3COM
00:09:6E               Avaya
Interface        Enabled    Secure    Activated  CoS Mode
-------------    -------    -------   ---------  --------
gi1              Yes        Yes         Yes      all
gi2              Yes        Yes         No       src
gi3              No         No
...
```

36 Loopback Detection Commands

36.1 loopback-detection enable (Global)

Use the **loopback-detection enable** Global Configuration mode command to enable the Loopback Detection (LBD) feature globally. Use the **no** form of this command to disable the Loopback Detection feature.

Syntax

loopback-detection enable

no loopback-detection enable

Default Configuration

Loopback Detection is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables the Loopback Detection feature globally. Use the **loopback-detection enable** Interface Configuration mode command to enable Loopback Detection on an interface.

Example

The following example enables the Loopback Detection feature on the device.

```
Console(config)# loopback-detection enable
```

36.2 loopback-detection enable (Interface)

Use the **loopback-detection enable** Interface Configuration (Ethernet) mode command to enable the Loopback Detection (LBD) feature on an interface. Use the **no** form of this command to disable the Loopback Detection feature on the interface.

Syntax

loopback-detection enable

no loopback-detection enable

Default Configuration

Loopback Detection is disabled on an interface.

Command Mode

Interface Configuration (Ethernet) mode

User Guidelines

This command enables Loopback Detection on an interface. Use the **loopback-detection enable** Global Configuration command to enable Loopback Detection globally.

LBD packets are sent only if the interface spanning tree state is Forwarding.

If the STP mode is MSTP, Loopback Detection can be enabled only on STP-disabled interfaces.

The interface should be a VLAN member of its PVID; otherwise, LBD packets are not trapped by the device.

The interface should be configured with Acceptable-Frame-Type Tagged-Only, otherwise LBD packets are not trapped by the device.

LBD packets are subject to the user's MAC ACLs. Therefore, an LBD packet can be discarded by an explicit deny rule, and by an implicit Deny All rule.

Example

The following example enables the Loopback Detection feature on gigabitethernet port `fe1/0/1`6.

```
Console(config)# interface fe1/0/16
Console(config-if)# loopback-detection enable
```

36.3 loopback-detection mode

Use the **loopback-detection mode** Global Configuration mode command to set the Loopback Detection mode. Use the **no** form of this command to restore the default configuration.

Syntax

loopback-detection mode *{src-mac-addr | base-mac-addr}*

no loopback-detection mode

Parameters

- **src-mac-addr**—Specifies that the LBD packet destination MAC address is the source interface MAC address.
- **base-mac-addr**—Specifies that the LBD packet destination MAC address is the device base MAC address.

Default Configuration

Src-mac-addr is the default.

Command Mode

Global Configuration mode

Example

The following example sets the Loopback Detection mode to a **src-mac-addr**.

```
Console(config)# loopback-detection mode src-mac-addr
```

36.4 loopback-detection interval

Use the **loopback-detection interval** Global Configuration mode command to set the time interval between LBD packets. Use the **no** form of this command to restore the default configuration.

Syntax

loopback-detection interval *seconds*

no loopback-detection interval

Parameters

seconds—Specifies the time interval in seconds between LBD packets. (Range: 30–60 seconds)

Default Configuration

The default time interval between LBD packets is 30 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command is not relevant for spanning-tree BPDU handling.

Example

The following example sets the time interval between LBD packets to 45 seconds.

```
Console(config)# loopback-detection interval 45
```

36.5 show loopback-detection

Use the **show loopback-detection** EXEC mode command to display information about Loopback Detection.

Syntax

show loopback-detection *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following example display information about Loopback Detection.

```
Console# show loopback-detection

Loopback detection: Enabled
Mode: src-mac-addr
LBD packets interval: 30 Seconds

Interface     Loopback Detection
---------     ------------------
fe1/0/11      Enabled
fe1/0/12      Enabled
fe1/0/13      Disabled
fe1/0/14      Disabled
fe1/0/15      Disabled
```

37 DHCP Snooping and ARP Inspection Commands

37.1 ip dhcp snooping

Use the **ip dhcp snooping** Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping

no ip dhcp snooping

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled by using the **ip dhcp snooping vlan** Global Configuration mode command.

Example

The following example enables DHCP Snooping on the device.

```
Console(config)# ip dhcp snooping
```

37.2 ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the **no** form of this command to disable DHCP Snooping on a VLAN.

Syntax

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID.

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode
Global Configuration mode

User Guidelines
DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example
The following example enables DHCP Snooping on VLAN 21.

```
Console(config)# ip dhcp snooping vlan 21
```

37.3 ip dhcp snooping trust

Use the **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to restore the default configuration.

Syntax
ip dhcp snooping trust

no ip dhcp snooping trust

Default Configuration
The interface is untrusted.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example
The following example configures fe1/0/15 as trusted for DHCP Snooping.

```
Console(config)# interface fe1/0/15
Console(config-if)# ip dhcp snooping trust
```

37.4 ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the **no** form of this command to drop these packets from an untrusted port.

Syntax
ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Default Configuration
DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode
Global Configuration mode

Example
The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
Console(config)# ip dhcp snooping information option allowed-untrusted
```

37.5 ip dhcp snooping verify
Use the **ip dhcp snooping verify** Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the **no** form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

Syntax
ip dhcp snooping verify

no ip dhcp snooping verify

Default Configuration
The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

Command Mode
Global Configuration mode

Example
The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
Console(config)# ip dhcp snooping verify
```

37.6 ip dhcp snooping database
Use the **ip dhcp snooping database** Global Configuration mode command to enable the DHCP Snooping binding database file. Use the **no** form of this command to delete the DHCP Snooping binding database file.

Syntax
ip dhcp snooping database

no ip dhcp snooping database

Default Configuration
The DHCP Snooping binding database file is not defined.

Command Mode
Global Configuration mode

User Guidelines
The DHCP Snooping binding database file resides on Flash.

To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured.

The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example
The following example enables the DHCP Snooping binding database file.

```
Console(config)# ip dhcp snooping database
```

37.7 ip dhcp snooping database update-freq
Use the **ip dhcp snooping database update-freq** Global Configuration mode command to set the update frequency of the DHCP Snooping binding database file. Use the **no** form of this command to restore the default configuration.

Syntax
ip dhcp snooping database update-freq *seconds*

no ip dhcp snooping database update-freq

Parameters
seconds—Specifies the update frequency in seconds. (Range: 600–86400)

Default Configuration
The default update frequency value is 1200 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the DHCP Snooping binding database file update frequency to 1 hour.

```
Console(config)# ip dhcp snooping database update-freq 3600
```

37.8 ip dhcp snooping binding

Use the **ip dhcp snooping binding** Privileged EXEC mode command to configure the DHCP Snooping binding database and add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

Syntax

ip dhcp snooping binding *mac-address vlan-id ip-address interface-id* ***expiry*** *{seconds* | ***infinite****}*

no ip dhcp snooping binding mac-address vlan-id

Parameters

- **mac-address**— pecifies a MAC address.
- **vlan-id**—Specifies a VLAN number.
- **ip-address**—Specifies an IP address.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **expiry** *seconds*—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967295)
- **expiry** ***infinite***—Specifies infinite lease time.

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry is displayed in the show commands as a DHCP Snooping entry.

The user cannot delete dynamic temporary entries for which the IP address is 0.0.0.0.

Example

The following example adds a binding entry to the DHCP Snooping binding database.

```
Console# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 fe1/0/15
expiry 900
```

37.9 clear ip dhcp snooping database

Use the **clear ip dhcp snooping database** Privileged EXEC mode command to clear the DHCP Snooping binding database.

Syntax

clear ip dhcp snooping database

Command Mode
Privileged EXEC mode

Example
The following example clears the DHCP Snooping binding database.

```
Console# clear ip dhcp snooping database
```

37.10 show ip dhcp snooping
Use the **show ip dhcp snooping** EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

Syntax
show ip dhcp snooping *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the DHCP snooping configuration.

```
console# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds

 Interface    Trusted
----------- ------------
fe1/0/11          Yes
fe1/0/12          Yes
```

37.11 show ip dhcp snooping binding
Use the **show ip dhcp snooping binding** User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

Syntax

show ip dhcp snooping binding ***[mac-address*** *mac-address]* ***[ip-address*** *ip-address]* ***[vlan*** *vlan-id]* *[interface-id]*

Parameters

- **mac-address mac-address**—Specifies a MAC address.
- **ip-address ip-address**—Specifies an IP address.
- **vlan vlan-id**—Specifies a VLAN ID.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.-

```
Console# show ip dhcp snooping binding

Update frequency: 1200
Total number of binding: 2

Mac Address       IP           Lease      Type         VLAN    Interface
                  Address      (sec)
------------      ---------    -------    --------     ----    ---------
0060.704C.73FF    10.1.8.1     7983       snooping     3       fe1/0/121
0060.704C.7BC1    10.1.8.2     92332      snooping     3       fe1/0/122
                                          (s)
```

37.12 ip source-guard

Use the **ip source-guard** Interface Configuration (Ethernet, Port-channel) mode command to enable IP Source Guard on an interface. Use the **no** form of this command to disable IP Source Guard on an interface.

Syntax

ip source-guard

no ip source-guard

Default Configuration

IP source guard is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

IP Source Guard must be enabled globally before enabling IP Source Guard on an interface.

IP Source Guard is active only on DHCP snooping untrusted interfaces, and if at least one of the interface VLANs are DHCP snooping enabled.

Example
The following example enables IP Source Guard on `fe1/0/15`.

```
Console(config)# interface fe1/0/15
Console(config-if)# ip source-guard
```

37.13 ip source-guard binding
Use the **ip source-guard binding** Global Configuration mode command to configure the static IP source bindings on the device. Use the **no** form of this command to delete the static bindings.

Syntax
ip source-guard binding *mac-address vlan-id ip-address* {*interface-id*}

no ip source-guard binding *mac-address vlan-id*

Parameters
- **mac-address**—Specifies a MAC address.
- **vlan-id**—Specifies a VLAN number.
- **ip-address**—Specifies an IP address.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Default Configuration
No static binding exists.

Command Mode
Global Configuration mode

User Guidelines
The device currently supports filtering that is based only on the source IP address. In future, the device might supports filtering mode that is based on the MAC address and IP source address. Currently the MAC address field is an informative field.

Example
The following example configures the static IP source bindings.

```
Console(config)# ip source-guard binding 0060.704C.73FF 23 176.10.1.1
fe1/0/15
```

37.14 ip source-guard tcam retries-freq
Use the **ip source-guard tcam retries-freq** Global Configuration mode command to set the frequency of retries for TCAM resources for inactive IP Source Guard addresses. Use the **no** form of this command to restore the default configuration.

Syntax

ip source-guard tcam retries-freq {*seconds* | ***never***}

no ip source-guard tcam retries-freq

Parameters

- **seconds**—Specifies the retries frequency in seconds. (Range: 10–600)
- **never**—Disables automatic searching for TCAM resources.

Default Configuration

The default retries frequency is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses. Use this command to change the search frequency or to disable automatic retries for TCAM space.

The **ip source-guard tcam locate** Privileged EXEC mode command manually retries locating TCAM resources for the inactive IP Source Guard addresses.

The **show ip source-guard inactive** EXEC mode command displays the inactive IP Source Guard addresses.

Example

The following example sets the frequency of retries for TCAM resources to 2 minutes.

```
Console(config)# ip source-guard tcam retries-freq 120
```

37.15 ip source-guard tcam locate

Use the **ip source-guard tcam locate** Privileged EXEC mode command to manually retry to locate TCAM resources for inactive IP Source Guard addresses.

Syntax

ip source-guard tcam locate

Command Mode

Privileged EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Execute the **ip source-guard tcam retries-freq never** Global Configuration mode command to disable automatic retries for TCAM space, and then execute this command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

The **show ip source-guard inactive** EXEC mode command displays the inactive IP source guard addresses.

Example
The following example manually retries to locate TCAM resources.

```
Console# ip source-guard tcam locate
```

37.16 show ip source-guard configuration
Use the **show ip source-guard configuration** EXEC mode command to display the IP source guard configuration for all interfaces or for a specific interface.

Syntax
show ip source-guard configuration *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the IP Source Guard configuration.

```
Console# show ip source-guard configuration

IP source guard is globally enabled.

Interface                   State
---------                   -------
fe1/0/121                   Enabled
fe1/0/122                   Enabled
fe1/0/123                   Enabled
fe1/0/124                   Enabled
fe1/0/132                   Enabled
fe1/0/133                   Enabled
fe1/0/134                   Enabled
```

37.17 show ip source-guard status

Use the **show ip source-guard status** EXEC mode command to display the IP Source Guard status.

Syntax

show ip source-guard status [***mac-address*** *mac-address]* ***[ip-address*** *ip-address]* ***[vlan*** *vlan]* *[interface-id*

Parameters

- **mac-address mac-address**—Specifies a MAC address.
- **ip-address ip-address**—Specifies an IP address.
- **vlan vlan-id**—Specifies a VLAN ID.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

EXEC mode

Example

The following examples display the IP Source Guard status.

```
Console# show ip source-guard status
IP source guard is globally disabled.

Console# show ip source-guard status


Interface   Filter   Status     IP Address       MAC Address          VLAN    Type
-------     -----    -------    -----------      ---------------      ---     -----
fe1/0/12    IP       Active     10.1.8.1         0060.704C.73FF       3       DHCP
1           IP       Active     10.1.8.2         0060.704C.7BC1       3       DHCP
fe1/0/12    IP       Active     10.1.12.2        0060.704C.7BC3       4       DHCP
2           IP       Active     Deny all
fe1/0/12    IP       Active     10.1.8.218       0060.704C.7BAC       3       Static
3           IP       Inactive   10.1.8.32        0060.704C.83FF       3       DHCP
fe1/0/12    IP       Inactive
4           IP       Inactive
fe1/0/12    IP       Inactive
5
fe1/0/13
2
fe1/0/13
3
fe1/0/13
4
fe1/0/13
5
```

37.18 show ip source-guard inactive

Use the **show ip source-guard inactive** EXEC mode command to display the IP Source Guard inactive addresses.

Syntax

show ip source-guard inactive

Command Mode

EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every minute the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Use the **ip source-guard tcam retries-freq** Global Configuration mode command to change the retry frequency or to disable automatic retries for TCAM space.

Use the **ip source-guard tcam locate** Privileged EXEC mode command to manually retry locating TCAM resources for the inactive IP Source Guard addresses.

This command displays the inactive IP source guard addresses.

Example

The following example displays the IP source guard inactive addresses.

```
Console# show ip source-guard inactive

TBD: TCAM resources search frequency: 10 minutes

Interface    Filter    IP           MAC Address    VLAN    Type    Reason
                       Address
--------     -----     ---------    -----------    -----   ----    ----------
fe1/0/132    IP        10.1.8.32    0060.704C.8    3       DHCP    Resource
fe1/0/133    IP                     3FF                            Problem
fe1/0/134    I                                                     Trust port
                                                                   No snooping
                                                                   VLAN
```

37.19 ip arp inspection

Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

Syntax

ip arp inspection

no ip arp inspection

Default Configuration
ARP inspection is disabled.

Command Mode
Global Configuration mode

User Guidelines
Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

Example
The following example enables ARP inspection on the device.

```
Console(config)# ip arp inspection
```

37.20 ip arp inspection vlan
Use the **ip arp inspection vlan** Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the **no** form of this command to disable ARP inspection on a VLAN.

Syntax
ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Parameters
vlan-id—Specifies the VLAN ID.

Default Configuration
DHCP Snooping based ARP inspection on a VLAN is disabled.

Command Mode
Global Configuration mode

User Guidelines
This command enables ARP inspection on a VLAN based on the DHCP snooping database. Use the **ip arp inspection list assign** Global Configuration mode command to enable static ARP inspection.

Example
The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
Console(config)# ip arp inspection vlan 23
```

37.21 ip arp inspection trust

Use the **ip arp inspection trust** Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection trust

no ip arp inspection trust

Default Configuration

The interface is untrusted.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

The device does not check ARP packets that are received on the trusted interface; it only forwards the packets.

For untrusted interfaces, the device intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The device drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection log-buffer vlan** Global Configuration mode command.

Example

The following example configures `fe1/0/1`3 as a trusted interface.

```
Console(config)# interface fe1/0/13
Console(config-if)# ip arp inspection trust
```

37.22 ip arp inspection validate

Use the **ip arp inspection validate** Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection validate

no ip arp inspection validate

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address**: Compares the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- **Destination MAC address**: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- **IP addresses**: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

```
Console(config)# ip arp inspection validate
```

37.23 ip arp inspection list create

Use the **ip arp inspection list create** Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the **no** form of this command to delete the list.

Syntax

ip arp inspection list create *name*

no ip arp inspection list create *name*

Parameters

name—Specifies the static ARP binding list name. (Length: 1–32 characters)

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

Use the **ip arp inspection list assign** command to assign the list to a VLAN.

Example

The following example creates the static ARP binding list ‘servers’ and enters the ARP list configuration mode.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)#
```

37.24 ip mac

Use the **ip mac** ARP-list Configuration mode command to create a static ARP binding. Use the **no** form of this command to delete a static ARP binding.

Syntax

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Parameters

- **ip-address**—Specifies the IP address to be entered to the list.
- **mac-address**—Specifies the MAC address associated with the IP address.

Default Configuration

No static ARP binding is defined.

Command Mode

ARP-list Configuration mode

Example

The following example creates a static ARP binding.

```
Console(config)# ip arp inspection list create servers
Console(config-ARP-list)# ip 172.16.1.1 mac 0060.704C.7321
Console(config-ARP-list)# ip 172.16.1.2 mac 0060.704C.7322
```

37.25 ip arp inspection list assign

Use the **ip arp inspection list assign** Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the **no** form of this command to delete the assignment.

Syntax

ip arp inspection list assign *vlan-id name*

no ip arp inspection list assign *vlan-id*

Parameters

- **vlan-id**—Specifies the VLAN ID.
- **name**—Specifies the static ARP binding list name.

Default Configuration

No static ARP binding list assignment exists.

Command Mode

Global Configuration mode

Example
The following example assigns the static ARP binding list Servers to VLAN 37.

```
Console(config)# ip arp inspection list assign 37 servers
```

37.26 ip arp inspection logging interval
Use the **ip arp inspection logging interval** Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the **no** form of this command to restore the default configuration.

Syntax
ip arp inspection logging interval {*seconds* | ***infinite***}

no ip arp inspection logging interval

Parameters
- **seconds**—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- **infinite**—Specifies that SYSLOG messages are not generated.

Default Configuration
The default minimum ARP SYSLOG message logging time interval is 5 seconds.

Command Mode
Global Configuration mode

Example
The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
Console(config)# ip arp inspection logging interval 60
```

37.27 show ip arp inspection
Use the **show ip arp inspection** EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

Syntax
show ip arp inspection *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types:Ethernet port or Port-channel.

Command Mode
EXEC mode

Example
The following example displays the ARP inspection configuration.

```
console# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222  seconds

 Interface    Trusted
----------- -----------
fe1/0/11          Yes
fe1/0/12          Yes
```

37.28 show ip arp inspection list
Use the **show ip arp inspection list** Privileged EXEC mode command to display the static ARP binding list.

Syntax
show ip arp inspection list

Command Mode
Privileged EXEC mode

Example
The following example displays the static ARP binding list.

```
Console# show ip arp inspection list

List name: servers
Assigned to VLANs: 1,2

IP            ARP
-----------   --------------
172.16.1.1    0060.704C.7322
172.16.1.2    0060.704C.7322
```

37.29 show ip arp inspection statistics
Use the **show ip arp inspection statistics** EXEC command to display Statistics For The Following Types Of Packets That Have Been Processed By This Feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax
show ip arp inspection statistics ***[vlan*** *vlan-id]*

Parameters
vlan-id—Specifies VLAN ID.

Command Mode
EXEC mode

User Guidelines
To clear ARP Inspection counters use the **clear ip arp inspection statistics** CLI command. Counters values are kept when disabling the ARP Inspection feature.

Example

```
console# show ip arp inspection statistics

Vlan     Forwarded Packets        Dropped Packets     IP/MAC Failures
----     -----------------        ---------------     ---------------
2        1500                     100                 80
```

37.30 clear ip arp inspection statistics
Use the **clear ip arp inspection statistics** Privileged EXEC mode command to clear statistics ARP Inspection statistics globally.

Syntax
clear ip arp inspection statistics ***[vlan*** *vlan-id]*

Parameters
vlan-id—Specifies VLAN ID

Command Mode
Privileged EXEC mode

Example

```
console# clear ip arp inspection statistics
```

38 IP Addressing Commands

38.1 ip address

Use the **ip address** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to define an IP address for an interface. Use the **no** form of this command to remove an IP address definition.

Syntax

If the product is in router mode (Layer 3).

ip address *ip-address* {*mask* | /*prefix-length*}

no ip address [*ip-address*]

If the product is in switch mode (Layer 2).

ip address *ip-address* {*mask* | /*prefix-length*} [**default-gateway** *ip-address*]

no ip address [*ip-address*]

If the product can only be switch mode (Layer 2) and supports a single IP address:

ip address *ip-address* {*mask* | /*prefix-length*} [**default-gateway** *ip-address*]

no ip address

Parameters

- **ip-address**—Specifies the IP address.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix.The prefix length must be preceded by a forward slash (/). (Range: 8–30)
- **default-gateway** *ip-address*—Specifies the default gateway IP address.

Default Configuration

No IP address is defined for interfaces.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

Defining a static IP address on an interface implicitly removes the DHCP client configuration on the interface.

If the device is in router mode, it supports multiple IP addresses:

- The product supports up to IP addresses.
- The IP addresses must be from different IP subnets. When adding an IP address from a subnet that already exists in the list, the new IP address replaces the existing IP address from that subnet.

If the IP address is configured in Interface context, the IP address is bound to the interface in that context.

If a static IP address is already defined, the user must do **no IP address** in the relevant interface context before changing the IP address.

If a dynamic IP address is already defined, the user must do **no ip address** in the relevant interface context before configuring another dynamic IP address.

The Interface context may be a port, LAG or VLAN, depending on support that is defined for the product.

Example

The following example configures VLAN 1 with IP address 131.108.1.27 and subnet mask 255.255.255.0.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 131.108.1.27 255.255.255.0
```

38.2 ip address dhcp

Use the **ip address dhcp** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to acquire an IP address for an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP) server. Use the **no** form of this command to release an acquired IP address.

Syntax

ip address dhcp

no ip address dhcp

Parameters

N/A

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command enables any interface to dynamically learn its IP address by using the DHCP protocol.

DHCP client configuration on an interface implicitly removes the static IP address configuration on the interface.

If the device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

The **no ip address dhcp** command releases any IP address that was acquired, and sends a DHCPRELEASE message.

Example

The following example acquires an IP address for `fe1/0/116` from DHCP.

```
switchxxxxxx(config)# interface fe1/0/116
```

```
switchxxxxxx(config-if)# ip address dhcp
```

38.3 renew dhcp

Use the **renew dhcp** Privileged EXEC mode command to renew an IP address that was acquired from a DHCP server for a specific interface.

Syntax

renew dhcp *{interface-id} [***force-autoconfig***]*

Parameters

- **interface-id**—Only required in routing mode (Layer 3). Specifies an interface ID (Ethernet port, Port-channel or VLAN).
- **force-autoconfig** - If the DHCP server holds a DHCP option 67 record for the assigned IP address, the record overwrites the existing device configuration.

Command Mode

Privileged EXEC mode

User Guidelines

Note the following:

- When the device is in Layer 2 (switch mode), interface-id is not required..
- This command does not enable DHCP on an interface. If DHCP is not enabled on the requested interface, the command returns an error message.
- If DHCP is enabled on the interface and an IP address was already acquired, the command tries to renew that IP address.
- If DHCP is enabled on the interface and an IP address has not yet been acquired, the command initiates a DHCP request.

Example

The following example renews an IP address that was acquired from a DHCP server for VLAN 19. This assumes that the device is in Layer 3.

```
switchxxxxxx# renew dhcp vlan 19
```

38.4 ip default-gateway

The **ip default-gateway** Global Configuration mode command defines a default gateway (device). Use the **no** form of this command to restore the default configuration.

Syntax

ip default-gateway *ip-address*

no ip default-gateway

Parameters

ip-address—Specifies the default gateway IP address.

Command Mode
Global Configuration mode

Default Configuration
No default gateway is defined.

Example
The following example defines default gateway 192.168.1.1.

```
switchxxxxxx(config)# ip default-gateway 192.168.1.1
```

38.5 show ip interface
Use the **show ip interface** EXEC mode command to display the usability status of configured IP interfaces.

Syntax
show ip interface *[interface-id]*

Parameters
interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration
All IP addresses.

Command Mode
EXEC mode

Example
The following example displays the configured IP interfaces and their types when the device is in Switch mode.

```
switchxxxxxx# show ip interface
 Gateway IP Address       Activity status      Type
---------------------- ---------------------- --------
10.5.234.254            Active                 static
   IP Address        I/F      Type       Status
------------------- --------- ----------- -----------
10.5.234.207/24     vlan 1    Static      Valid
```

38.6 arp
Use the **arp** Global Configuration mode command to add a permanent entry to the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove an entry from the ARP cache.

Syntax

arp *ip-address mac-address [interface-id]]*

no arp *ip-address*

Parameters

- **ip-address**—IP address or IP alias to map to the specified MAC address.
- **mac-address**—MAC address to map to the specified IP address or IP alias.
- **interface-id**—Address pair is added for specified interface that can be Ethernet port, Port-channel or VLAN.

Command Mode

Global Configuration mode

Default Configuration

No permanent entry is defined.

If no interface ID is entered, address pair is relevant to all interfaces.

User Guidelines

The software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware (MAC) addresses. Because most hosts support dynamic address resolution, static ARP cache entries generally do not need to be specified.

Example

The following example adds IP address 198.133.219.232 and MAC address 00:00:0c:40:0f:bc to the ARP table.

```
switchxxxxxx(config)# arp 198.133.219.232 00:00:0c:40:0f:bc fe1/0/16
```

38.7 arp timeout (Global)

Use the **arp timeout** Global Configuration mode command to set the time interval during which an entry remains in the ARP cache. Use the **no** form of this command to restore the default configuration.

Syntax

arp timeout *seconds*

no arp timeout

Parameters

seconds—Specifies the time interval (in seconds) during which an entry remains in the ARP cache. (Range: 1–40000000)

Default Configuration

The default ARP timeout is 60000 seconds in Router mode, and 300 seconds in Switch mode.

Command Mode

Global Configuration mode

Example
The following example configures the ARP timeout to 12000 seconds.

```
switchxxxxxx(config)# arp timeout 12000
```

38.8 arp timeout
Use the **arp timeout** inTerface Configuration command to configure how long an entry remains in the ARP cache for specific interface. Use the **no** form of this command restore the default value.

Syntax
arp timeout *seconds*

no arp timeout

Parameters
seconds—Time (in seconds) that an entry remains in the ARP cache. It is recommended not to set it to less than 3600. (Range: 1–40000000)

Default
Defined by the **arp timeout** Global Configuration command

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
This configuration can be applied only if at least one IP address is defined on specific interface.

Example

```
switchxxxxxx (config)# interface vlan 1
switchxxxxxx(config-if)# arp timeout 12000
```

38.9 ip arp proxy disable
Use the **ip arp proxy disable** Global Configuration mode command to globally disable proxy Address Resolution Protocol (ARP). Use the **no** form of this command reenable proxy ARP.

Syntax
ip arp proxy disable

no ip arp proxy disable

Parameters
N/A

Default
Enabled by default.

Command Mode
Global Configuration mode

User Guidelines

T his command overrides any proxy ARP interface configuration. **Example**
The following example globally disables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config)# ip arp proxy disable
```

38.10 ip proxy-arp
Use the **ip proxy-arp** Interface Configuration mode command to enable an ARP proxy on specific interfaces. Use the **no** form of this command disable it.

Syntax
ip proxy-arp

no ip proxy-arp

Default Configuration
ARP Proxy is disabled.

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
This configuration can be applied only if at least one IP address is defined on a specific interface.

Example
The following example enables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config-if)# ip proxy-arp
```

38.11 clear arp-cache
Use the **clear arp-cache** Privileged EXEC mode command to delete all dynamic entries from the ARP cache.

Syntax
clear arp-cache

Command Mode
Privileged EXEC mode

Example
The following example deletes all dynamic entries from the ARP cache.

```
switchxxxxxx# clear arp-cache
```

38.12 show arp
Use the **show arp** Privileged EXEC mode command to display entries in the ARP table.

Syntax
show arp ***[ip-address*** *ip-address]* ***[mac-address*** *mac-address] [interface-id]*

Parameters
- **ip-address** *ip-address*—Specifies the IP address.
- **mac-address** *mac-address*—Specifies the MAC address.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode
Privileged EXEC mode

User Guidelines
Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

If an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

Example
The following example displays entries in the ARP table.

```
switchxxxxxx# show arp
ARP timeout: 80000 Seconds

VLAN      Interface   IP Address   HW Address          Status
-------   ---------   ----------   -------------       -------
VLAN 1    fe1/0/11    10.7.1.102   00:10:B5:04:DB:4B   Dynamic
VLAN 1    fe1/0/12    10.7.1.135   00:50:22:00:2A:A4   Static
```

38.13 show arp configuration
Use the **show arp configuration** privileged EXEC command to display the global and interface configuration of the ARP protocol.

Syntax
show arp configuration

Parameters
This command has no arguments or key words.

Command Mode
Privileged EXEC mode

Example

```
switchxxxxxx# show arp configuration
Global configuration:
   ARP Proxy: enabled
   ARP timeout:    80000 Seconds
Interface configuration:
g2:
   ARP Proxy: disabled
   ARP timeout:60000 Seconds
VLAN 1:
   ARP Proxy: enabled
   ARP timeout:70000 Seconds
VLAN 2:
   ARP Proxy: enabled
   ARP timeout:80000 Second (Global)
```

38.14 interface ip
Use the **interface ip** Global Configuration mode command to enter the IP Interface Configuration mode.

Syntax
interface ip-*address*

Parameters
ip-address—Specifies one of the IP addresses of the device.

Command Mode
Global Configuration mode

Example
The following example enters the IP interface configuration mode.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)#
```

38.15 directed-broadcast

Use the **directed-broadcast** IP Interface Configuration mode command to enable the translation of a directed broadcast to physical broadcasts. Use the **no** form of this command to disable this function.

Syntax

directed-broadcast

no directed-broadcast

Default Configuration

Translation of a directed broadcast to physical broadcasts is disabled. All IP directed broadcasts are dropped.

Command Mode

IP Interface Configuration mode

Example

The following example enables the translation of a directed broadcast to physical broadcasts.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)# directed-broadcast
```

38.16 broadcast-address

Use the **broadcast-address** IP Interface Configuration mode command to define a broadcast address for an interface. Use the **no** form of this command to restore the default IP broadcast address.

Syntax

broadcast-address *{255.255.255.255 | 0.0.0.0}*

no broadcast-address

Parameters

- **255.255.255.255**—Specifies 255.255.255.255 as the broadcast address.
- **0.0.0.0**—Specifies 0.0.0.0 as the broadcast address.

Default Configuration

The default broadcast address is 255.255.255.255.

Command Mode

IP Interface Configuration mode

Example

The following example enables the translation of a directed broadcast to physical broadcasts.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)# broadcast-address 255.255.255.255
```

38.17 ip helper-address

Use the **ip helper-address** Global Configuration mode command to enable the forwarding of UDP Broadcast packets received on an interface to a specific (helper) address. Use the **no** form of this command to disable the forwarding of broadcast packets to a specific (helper) address.

Syntax

ip helper-address {*ip-interface* | ***all}*** *address* [*udp-port-list*]

no ip helper-address {*ip-interface* | ***all}*** *address*

Parameters

- **ip-interface**—Specifies the IP interface.
- **all**—Specifies all IP interfaces.
- **address**—Specifies the destination broadcast or host address to which to forward UDP broadcast packets. A value of 0.0.0.0 specifies that UDP broadcast packets are not forwarded to any host.
- **udp-port-list**—Specifies the destination UDP port number to which to forward Broadcast packets. (Range: 1–65535). This can be a list of port numbers separated by spaces.

Default Configuration

Forwarding of UDP Broadcast packets received on an interface to a specific (helper) address is disabled.

If **udp-port-list** is not specified, packets for the default services are forwarded to the helper address.

Command Mode

Global Configuration mode

User Guidelines

This command forwards specific UDP Broadcast packets from one interface to another, by specifying a UDP port number to which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- IEN-116 Name Service (port 42)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

Many helper addresses may be defined. However, the total number of address-port pairs is limited to 128 for the device.

The setting of a helper address for a specific interface has precedence over the setting of a helper address for all the interfaces.

Forwarding of BOOTP/DHCP (ports 67, 68) cannot be enabled with this command. Use the DHCP relay commands to relay BOOTP/DHCP packets.

Example

The following example enables the forwarding of UDP Broadcast packets received on all interfaces to the UDP ports of a destination IP address and UDP port 1 and 2.

```
switchxxxxxx(config)# ip helper-address all 172.16.9.9 49 53 1 2
```

38.18 show ip helper-address

Use the **show ip helper-address** Privileged EXEC mode command to display the IP helper addresses configuration on the system.

Syntax

show ip helper-address

Parameters

This command has no arguments or key words.

Command Mode

Privileged EXEC mode

Example

The following example displays the IP helper addresses configuration on the system.

```
switchxxxxxx# show ip helper-address

Interface           Helper Address        UDP Ports
------------        --------------        ------------------------
192.168.1.1         172.16.8.8            37, 42, 49, 53, 137, 138
192.168.2.1         172.16.9.9            37, 49
```

38.19 source-precedence

Use the **source-precedence** IP Interface Configuration mode command to define a preference for an IP address as a source IP address for DHCP relayed messages on an interface. Use the **no** form of this command to restore the default configuration.

This can be used in Router mode only.

Syntax

source-precedence

no source-precedence

Default Configuration
Source precedence is not defined for the address.

Command Mode
IP Interface Configuration mode

User Guidelines
To use this command, you must put the switch into routing mode using the set system mode command.

For relayed DHCP messages, the source IP address selected is:

1. The lowest of the IP addresses defined as source-precedence IP addresses.
2. The lowest of the IP addresses if there are no source-precedence IP addresses.

Example
The following example defines a preference for an IP address as a source IP address for DHCP relayed messages on an interface.

```
switchxxxxxx(config-ip)# source-precedence
```

38.20 ip domain lookup
Use the **ip domain lookup** Global Configuration mode command to enable the IP Domain Name System (DNS)-based host name-to-address translation. Use the **no** form of this command to disable DNS-based host name-to-address translation.

Syntax
ip domain lookup

no ip domain lookup

Default Configuration
Enabled.

Command Mode
Global Configuration mode

Example
The following example enables DNS-based host name-to-address translation.

```
switchxxxxxx(config)# ip domain lookup
```

38.21 ip domain name
Use the **ip domain name** Global Configuration mode command to define a default domain name used by the software to complete unqualified host names (names without a dotted-decimal domain name). Use the **no** form of this command to remove the default domain name.

Syntax

ip domain name *name*

no ip domain name

Parameters

name—Specifies the default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters)

Default Configuration

A default domain name is not defined.

Command Mode

Global Configuration mode

User Guidelines

Domain names and host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

The maximum size of each domain level is 63 characters. The maximum name size is 158 bytes.

Example

The following example defines the default domain name as ‘www.website.com’.

```
switchxxxxxx(config)# ip domain name www.website.com
```

38.22 ip name-server

Use the **ip name-server** Global Configuration mode command to define the available name servers. Use the **no** form of this command to remove a name server.

Syntax

ip name-server *{server1-ip-address} [server-address2 … server-address8]*

no ip name-server [*server-address … server-address8*]

Parameters

server-address—IP addresses of the name server. Up to 8 servers can be defined in one command or by using multiple commands. The IP address can be an IPv4 address, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

No name server IP addresses are defined.

Command Mode

Global Configuration mode

User Guidelines

The preference of the servers is determined by the order in which they were entered.

Up to 8 servers can be defined using one command or using multiple commands.

Example
The following example defines the available name server.

```
switchxxxxxx(config)# ip name-server 176.16.1.18
```

38.23 ip host
Use the **ip host** Global Configuration mode command to define the static host name-to-address mapping in the host cache. Use the **no** form of this command to remove the static host name-to-address mapping.

Syntax
ip host *name address* [*address2 address3 address4*]

no ip host *name*

Parameters
- **name**—Specifies the host name. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters)
- **address**—Specifies the associated IP address. Up to 4 addresses can be defined separated by blanks.

Default Configuration
No host is defined.

Command Mode
Global Configuration mode

User Guidelines
Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.

Example
The following example defines a static host name-to-address mapping in the host cache.

```
switchxxxxxx(config)# ip host accounting.website.com 176.10.23.1
```

38.24 clear host
Use the **clear host** Privileged EXEC mode command to delete entries from the host name-to-address cache.

Syntax
clear host *{name | *}*

Parameters

- **name**—Specifies the host entry to remove. (Length: 1–158 characters. Maximum label length: of each domain level is 63 characters)
- * —Removes all entries.

Command Mode

Privileged EXEC mode

Example

The following example deletes all entries from the host name-to-address cache.

```
switchxxxxxx# clear host *
```

38.25 clear host dhcp

Use the **clear host dhcp** Privileged EXEC mode command to delete entries from the host name-to-address mapping received from the Dynamic Host Configuration Protocol (DHCP) server.

Syntax

clear host dhcp *{name | *}*

Parameters

- **name** —Specifies the host entry to remove. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters)
- *—Removes all entries.

Command Mode

Privileged EXEC mode

User Guidelines

This command deletes the host name-to-address mapping temporarily until the next refresh of the IP addresses.

Example

The following example deletes all entries from the host name-to-address mapping received from DHCP.

```
switchxxxxxx# clear host dhcp *
```

38.26 show hosts

Use the **show hosts** EXEC mode command to display the default domain name, the list of name server hosts, the static and the cached list of host names and addresses.

Syntax

show hosts *[name]*

Parameters

name—Specifies the host name. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters).

Command Mode

EXEC mode

Example

The following example displays host information.

```
switchxxxxxx#  show hosts
System name: Device
Default domain is gm.com, sales.gm.com, usa.sales.gm.com(DHCP)
Name/address lookup is enabled
Name servers (Preference order): 176.16.1.18 176.16.1.19
Configured host name-to-address mapping:

Host                                IP Addresses
-----------------                   --------------------------
accounting.gm.com                   176.16.8.8 176.16.8.9(DHCP)
                                    2002:0:130F::0A0:1504:0BB4

Cache: TTL (Hours)

Host              Total   Elapsed   Type     IP Addresses
--------------    -----   -------   ----     -------------
www.stanford.edu  72      3         IP       171.64.14.203
```

39 IPv6 Addressing Commands

39.1 ipv6 enable

Use the **ipv6 enable** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to enable the IPv6 addressing mode on an interface. Use the **no** form of this command to disable the IPv6 addressing mode on an interface.

Syntax

ipv6 enable ***[no-autoconfig]***

no ipv6 enable

Parameters

no-autoconfig—Enables processing of IPv6 on an interface without the stateless address autoconfiguration procedure. This procedure assigns link-local addresses.

Default Configuration

IPv6 addressing is disabled.

Unless you are using the no-autoconfig parameter, when the interface is enabled, stateless address autoconfiguration procedure is enabled.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

This command automatically configures an IPv6 link-local Unicast address on the interface, while also enabling the interface for IPv6 processing. The **no ipv6 enable** command removes the entire IPv6 interface configuration.

To enable stateless address autoconfiguration on an enabled IPv6 interface, use the ipv6 address autoconfig command.

Example

The following example enables VLAN 1 for the IPv6 addressing.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 enable
```

39.2 ipv6 address autoconfig

Use the **ipv6 address autoconfig** Interface Configuration mode command to enable automatic configuration of IPv6 addresses, using stateless autoconfiguration on an interface. Addresses are configured depending on the prefixes received in Router Advertisement messages. Use the **no** form of this command to disable address autoconfiguration on the interface.

Syntax

ipv6 address ***autoconfig***

no ipv6 address ***autoconfig***

Parameters

N/A

Default Configuration

Address autoconfiguration is enabled on the interface, no addresses are assigned by default.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode.

User Guidelines

When **address autoconfig** is enabled, the router solicitation ND procedure is initiated to discover a router and assign IP addresses to the interface, based on the advertised on-link prefixes.

When disabling address autoconfig, automatically generated addresses that were assigned to the interface are removed.

The default state of the address autoconfig is **enabled**. Use the **ipv6 enable no-autoconfig** command to enable an IPv6 interface without address autoconfig.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address autoconfig
```

39.3 ipv6 icmp error-interval

Use the **ipv6 icmp error-interval** Global Configuration mode command to configure the rate limit interval and bucket size parameters for IPv6 Internet Control Message Protocol (ICMP) error messages. Use the **no** form of this command to return the interval to its default setting.

Syntax

ipv6 icmp error-interval *milliseconds [bucketsize]*

no ipv6 icmp error-interval

Parameters

- **milliseconds**—The time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0–2147483647 with a default of 100 milliseconds. Setting milliseconds to 0 disables rate limiting. (Range: 0–2147483647)
- **bucketsize**—(Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1–200 with a default of 10 tokens.

Default Configuration

The default interval is 100ms and the default bucketsize is 10 i.e. 100 ICMP error messages per second.

Command Mode
Global Configuration mode

User Guidelines
To set the average ICMP error rate limit, calculate the interval with the following formula:

Average Packets Per Second = (1/ interval) * bucket size

Example

```
switchxxxxxx(config)# ipv6 icmp error-interval 123 45
```

39.4 show ipv6 icmp error-interval

Use the **show ipv6 error-interval** command in the EXEC mode to display the IPv6 ICMP error interval.

Syntax
show ipv6 icmp error-interval

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example

```
switchxxxxxx#  show ipv6 icmp error-interval
Rate limit interval: 100 ms
Bucket size: 10 tokens
```

39.5 ipv6 address

Use the **ipv6 address** Interface Configuration mode command to configure an IPv6 address for an interface. Use the **no** form of this command to remove the address from the interface.

Syntax
ipv6 address *ipv6-address/prefix-length* ***[eui-64]*** ***[anycast]***

no ipv6 address *[ipv6-address/prefix-length]* ***[link-local]*** ***[eui-64]***

Parameters
- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

- **prefix-length**—Specifies the length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal.
- **eui-64**—(Optional) Builds an interface ID in the low order 64 bits of the IPv6 address based on the interface MAC address.
- **anycast**—(Optional) Indicates that this address is an anycast address.
- **prefix-length**—3–128(64 when the **eui-64** parameter is used).
- **link-local**—Use the link-local address.

Default Configuration
No IP address is defined for the interface.

Command Mode
Interface configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
If the value specified for the /prefix-length argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the **no IPv6 address** command without arguments removes all manually configured IPv6 addresses from an interface, including link-local manually-configured addresses.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 3000::123/64 eui-64 anycast
```

39.6 ipv6 address link-local

Use the **ipv6 address link-local** command to configure an IPv6 link-local address for an interface. Use the **no** form of this command to return to the default link-local address on the interface.

Syntax
ipv6 address *ipv6-address /prefix-length* **link-local**

no ipv6 address [i*pv6-address /prefix-length* **link-local]**

Parameters
- **ipv6-address**—Specifies the IPv6 network assigned to the interface.This argument must be in the format documented in RFC 2373, where the address is specified in hexadecimals using 16-bit values between colons.
- **prefix-length**—Specifies the length of the IPv6 prefix. A decimal value indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark (/) must precede the decimal. Only 64-bit length is supported, according to IPv6 over Ethernet's well-known practice

Default Configuration
IPv6 is enabled on the interface, the link-local address of the interface is FE80::EUI64 (interface MAC address).

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines
Using the **no ipv6 link-local address** command removes the manually configured link-local IPv6 address from an interface. Multiple IPv6 addresses can be configured per interface, but only one link-local address. When the **no ipv6 link-local address** command is used, the interface is reconfigured with the standard link-local address (the same IPv6 link-local address that is set automatically when the **enable ipv6** command is used). The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface. To manually specify a link-local address to be used by an interface, use the **ip**v6 link-local address command. The system supports only 64 bits prefix length for link-local addresses.

Example

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address fe80::123/64 link-local
```

39.7 ipv6 unreachables
Use the **ipv6 unreachables** Interface Configuration mode command to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface. Use the **no** form of this command To prevent the generation of unreachable messages.

Syntax
ipv6 unreachables

no ipv6 unreachables

Parameters
N/A

Default Configuration
ICMP unreachable messages are sent by default.

Command Mode
Interface Configuration (Ethernet, VLAN, Port-channel) mode.

User Guidelines
When ICMP unreachable messages are enabled, when receiving a packet addressed to one of the interface's IP address with TCP/UDP port not assigned, the device sends ICMP unreachable messages.

Example

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# ipv6 unreachables
```

39.8 Ipv6 link-local default zone

Use the **Ipv6 link-local default zone** Interface command to configure an interface to egress a link-local packet without a specified interface or with the default zone 0. Use the **no** form of this command to return the default link-local interface to the default value.

Syntax

Ipv6 link-local default zone *{interface-id}*

no Ipv6 link-local default zone

Parameters

interface-id—Specifies the interface that is used as the egress interface for packets sent without a specified IPv6z interface identifier or with the default 0 identifier. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration

By default, **link local default zone** is disabled.

Command Mode

Interface configuration (Ethernet port, Port-channel or VLAN).

Example

```
switchxxxxxx(config)# ipv6 link-local default zone
```

39.9 ipv6 default-gateway

Use the **ipv6 default-gateway** Global Configuration mode command to define an IPv6 default gateway. Use the **no** form of this command To remove the default gateway.

Syntax

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

Parameters

ipv6-address—Specifies the IPv6 address of the next hop that can be used to reach the required network. When the IPv6 address is a link-local address (IPv6Z address), see IPv6z Address Conventions.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

Configuring a new default GW without deleting the previous configured information overwrites the previous configuration.

A configured default GW has a higher precedence over an automatically advertised (via router advertisement message).

Precedence takes effect after the configured default GW is reachable.

Reachability state is not verified automatically by the neighbor discovery protocol. Router reachability can be confirmed by either receiving a Router Advertisement message containing the router's MAC address or by manually configuring this using the ipv6 neighbor command. Another option to force reachability confirmation is to ping the router link-local address (this will initiate the neighbor discovery process).

If the egress interface is not specified, the default interface is selected. Specifying interface zone=0 is equal to not defining an egress interface.

Example

```
switchxxxxxx(config)# ipv6 default-gateway fe80::abcd
```

39.10 show ipv6 interface

Use the **show ipv6 interface** EXEC command mode to display the usability status of interfaces configured for IPv6.

Syntax

show ipv6 interface *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Default Configuration

Displays all IPv6 interfaces.

Command Mode

EXEC mode

User Guidelines

Use the s**how ipv6 neighbors** command in the privileged EXEC mode to display an IPv6 neighbor's discovery cache information.

Examples

Example 1- Show all IPv6 interfaces.

```
switchxxxxxx# show ipv6 interface
Interface    IP addresses                              Type
-----------  ----------------------------------------  ------------
VLAN 1       4004::55/64 [ANY]                         manual
```

```
VLAN 1       fe80::200:b0ff:fe00:0                  linklayer
VLAN 1       ff02::1                                linklayer
VLAN 1       ff02::77                               manual
VLAN 1       ff02::1:ff00:0                         manual
VLAN 1       ff02::1:ff00:1                         manual
VLAN 1       ff02::1:ff00:55                        manual
Default Gateway IP address     Type     Interface   State
----------------------------   -------- ---------   -----
fe80::77                       Static   VLAN 1      unreachable
fe80::200:cff:fe4a:dfa8        Dynamic  VLAN 1      stale
```

Example 2 - Show IPv6 interfaces on VLAN 15 where IPv6 is not enabled.

```
switchxxxxxx# show ipv6 interface Vlan 15
IPv6 is disabled
```

Example 3 - Show IPv6 interfaces on VLAN 15 where it is enabled.

```
switchxxxxxx# show ipv6 interface Vlan 1
Number of ND DAD attempts: 1
MTU size: 1500
Stateless Address Autoconfiguration state: enabled
ICMP unreachable message state: enabled
MLD version: 2
IP addresses                              Type         DAD State
----------------------------------------  ---------    -----------
4004::55/64 [ANY]                         manual       Active
fe80::200:b0ff:fe00:0                     linklayer    Active
ff02::1                                   linklayer    ------
ff02::77                                  manual       ------
ff02::1:ff00:0                            manual       ------
ff02::1:ff00:1                            manual       ------
ff02::1:ff00:55                           manual       ------
```

39.11 show IPv6 route

Use the **show ipv6 route** Exec mode command to display the current state of the IPv6 routing table.

Syntax

show ipv6 route

Parameters

N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example

```
switchxxxxxx#  show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisment
The number in the brackets is the metric.
S  ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite
ND ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec
L  2001::/64 is directly connected, g2 Lifetime Infinite
L  2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime 2147467 sec
L  3001::/64 is directly connected, VLAN 1 Lifetime Infinite
L  4004::/64 is directly connected, VLAN 1 Lifetime Infinite
L  6001::/64 is directly connected, g2 Lifetime Infinite
```

39.12 show ipv6 link-local default zone

Use the **show ipv6 link-local default zone** command in the EXEC mode to display the IPv6 link-local default zone.

Syntax
show ipv6 link-local default zone

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is defined on interface g1
```

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is not defined
```

39.13 ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** Interface Configuration (Ethernet, VLAN, Port-channel) mode command to configure the number of consecutive neighbor solicitation messages that are sent on an interface while Duplicate Address Detection (DAD) is performed on the unicast IPv6 addresses of the interface. Use the **no** form of this command to restore the number of messages to the default value.

Syntax

ipv6 nd dad attempts *attempts*

Parameters

attempts—Specifies the number of neighbor solicitation messages. A value of 0 disables DAD processing on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. (Range: 0–600)

Default Configuration

DAD on Unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode. It cannot be configured for a range of interfaces (range context).

User Guidelines

DAD verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while DAD is performed). DAD uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

An interface returning to the administrative Up state restarts DAD for all Unicast IPv6 addresses on the interface. While DAD is performed on the link-local address of an interface, the state of the other IPv6 addresses is still set to TENTATIVE. When DAD is completed on the link-local address, DAD is performed on the remaining IPv6 addresses.

When DAD identifies a duplicate address, the address state is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message is displayed.

All configuration commands associated with the duplicate address remain as configured, while the address state is set to DUPLICATE.

If the link-local address for an interface changes, DAD is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (DAD is performed only on the new link-local address).

Configuring a value of 0 with this command disables duplicate address detection processing on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. The default is 1 message.

Until the DAD process is completed, an IPv6 address is in the tentative state and cannot be used for data transfer. It is recommended to limit the configured value.

Example

The following example configures the number of consecutive neighbor solicitation messages sent during DAD processing to 2 on `fe1/0/19`.

```
switchxxxxxx (config)# interface fe1/0/19
switchxxxxxx (config-if)# ipv6 nd dad attempts 2
```

39.14 ipv6 host

Use the **ipv6 host** Global Configuration mode command to define a static host name-to-address mapping in the host name cache. Use the **no** form of this command to remove the host name-to-address mapping.

Syntax

ipv6 host *name ipv6-address1 [ipv6-address2...ipv6-address4]*

no ipv6 host name

Parameters

host name - Name of the host. (Range: 1–158 characters)

- **ipv6-address1**—Associated IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. When the IPv6 address is a link-local address (IPv6Z address), the outgoing interface name must be specified. See IPv6z Address Conventions.
- **ipv6-address2-4**—(Optional) Additional IPv6 addresses that may be associated with the host's name

Default Configuration

No host is defined.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# ipv6 host server 3000::a31b
```

39.15 ipv6 neighbor

Use the **ipv6 neighbor** command to configure a static entry in the IPv6 neighbor discovery cache. Use the **no** form of this command to remove a static IPv6 entry from the IPv6 neighbor discovery cache.

Syntax

ipv6 neighbor *ipv6_addr interface-id hw_addr*

no ipv6 neighbor *ipv6_addr interface-id*

Parameters

- **Ipv6_addr**—Specifies the Pv6 address to map to the specified MAC address.
- **interface-id**—Specifies the interface that is associated with the IPv6 address
- **hw_addr**—Specifies the MAC address to map to the specified IPv6 address.

Command Mode

Global Configuration mode

User Guidelines

The **IPv6 neighbor** command is similar to the arp command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

A new static neighbor entry with a global address can be configured only if a manually configured subnet already exists in the device.

Use the show ipv6 neighbors command to view static entries in the IPv6 neighbor discovery cache.

Example

```
switchxxxxxx(config)# ipv6 neighbor 3000::a31b vlan 1 001b.3f9c.84ea
```

39.16 ipv6 set mtu

Use the **ipv6 mtu** Privileged EXEC mode command to set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface. Use the default parameter to restore the default MTU size.

Syntax

ipv6 set mtu *{interface-id} {bytes* | ***default}***

Parameters

- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **bytes**—Specifies the MTU in bytes. Range is 1280-65535.
- **default**—Sets the default MTU size 1500 bytes. Minimum is 1280 bytes

Default Configuration

1500 bytes

Command Mode

Privileged EXEC mode

User Guidelines

This command is intended for debugging and testing purposes and should be used only by technical support personnel.

Example

```
switchxxxxxx# ipv6 set mtu fe1/0/11 default
```

39.17 ipv6 mld version

Use the **ipv6 mld version** Interface Configuration mode command to change the version of the Multicast Listener Discovery Protocol (MLD). Use the **no** form of this command to change to the default version.

Syntax

ipv6 mld version *{**1** | **2**}*

no ipv6 mld version

Parameters

- **1**—Specifies MLD version 1.
- **2**—Specifies MLD version 2.

Default Configuration

MLD version 1.

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld version 2
```

39.18 ipv6 mld join-group

Use the **ipv6 mld join-group** Interface Configuration mode command to configure MLD reporting for a specified group. Use the **no** form of this command to cancel reporting and leave the group.

Syntax

ipv6 mld join-group *group-address*

no ipv6 mld join-group *group-address*

Parameters

group-address—Specifies the IPv6 address of the Multicast group.

Default Configuration

N/A

Command Mode

Interface Configuration (Ethernet, VLAN, Port-channel) mode

User Guidelines

This command configures MLD reporting for a specified group. The packets that are addressed to a specified group address that will be passed to the client process in the device.

Example

The following example configures MLD reporting for specific groups:

```
switchxxxxxx(conf)#interface gi1
switchxxxxxx(conf-if)#ipv6 mld join-group ff02::10
```

39.19 show ipv6 neighbors

Use the **show ipv6 neighbors** Privileged EXEC mode command to display IPv6 neighbor discovery cache information.

Syntax

show ipv6 neighbors *{**static** | **dynamic**}[**ipv6-address** ipv6-address] [**mac-address** mac-address] [interface-id]*

Parameters

- **static**—Shows static neighbor discovery cash entries.
- **dynamic**—Shows dynamic neighbor discovery cash entries.
- **ipv6-address**—Shows the neighbor discovery cache information entry of a specific IPv6 address.
- **mac-address**—Shows the neighbor discovery cache information entry of a specific MAC address.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN.

Command Mode

Privileged EXEC mode

User Guidelines

Since the associated interface of a MAC address can be aged out from the FDB table, the Interface field can be empty.

When an ARP entry is associated with an IP interface that is defined on a port or port-channel, the VLAN field is empty.

The possible neighbor cash states are:

- **INCMP (Incomplete)**—Address resolution is being performed on the entry. Specifically, a Neighbor Solicitation has been sent to the solicited-node multicast address of the target, but the corresponding Neighbor Advertisement has not yet been received.
- **REACH (Reachable)**—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While REACHABLE, no special action takes place as packets are sent.
- **STALE**—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While stale, no action takes place until a packet is sent.
- **DELAY**—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly, and a packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a Neighbor Solicitation and change the state to PROBE.

- **PROBE**—A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every RetransTimer milliseconds until a reachability confirmation is received.

Example

```
switchxxxxxx# show ipv6 neighbors dynamic
Interface     IPv6 Address             HW Address         State*  Router
----------    -----------------------  -----------------  ------ ------
  VLAN 1      fe80::200:cff:fe4a:dfa8  00:00:0c:4a:df:a8  stale  yes
  VLAN 1      fe80::2d0:b7ff:fea1:264d 00:d0:b7:a1:26:4d  stale  no
*See State values above.
```

39.20 clear ipv6 neighbors

Use the **clear ipv6 neighbors** Privileged EXEC mode command to delete all entries in the IPv6 neighbor discovery cache, except for static entries.

Syntax

clear ipv6 neighbors

Parameters

This command has no keywords or arguments.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ipv6 neighbors
```

40 Tunnel Commands

40.1 interface tunnel

Use the **interface tunnel** Global Configuration mode command to enter the Interface Configuration (Tunnel) mode.

Syntax

interface tunnel *number*

Parameters

number—Specifies the tunnel index.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

The following example enters the Interface Configuration (Tunnel) mode.

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-tunnel)#
```

40.2 tunnel mode ipv6ip

Use the **tunnel mode ipv6ip** Interface Configuration (Tunnel) mode command to configure an IPv6 transition-mechanism global support mode. Use the **no** form of this command to remove an IPv6 transition mechanism.

Syntax

tunnel mode ipv6ip ***{isatap}***

no tunnel mode ipv6ip

Parameters

isatap—Enables an automatic IPv6 over IPv4 ISATAP tunnel.

Default Configuration

Disabled.

Command Mode

Interface Configuration (Tunnel) mode

User Guidelines

The system can be enabled to support ISATAP tunnels. When enabled, an automatic tunnel interface is created on each interface that is assigned an IPv4 address.

Note that on a specific interface (for example, port or VLAN), both native IPv6 and transition-mechanisms can coexist. The host implementation chooses the egress interface according to the scope of the destination IP address (such as ISATAP or native IPv6).

Example

The following example configures an ISATAP tunnel mechanism.

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-tunnel)# tunnel mode ipv6ip isatap
```

40.3 tunnel isatap router

Use the **tunnel isatap router** Interface Configuration (Tunnel) mode command to configure a global string that represents a specific automatic tunnel router domain name. Use the **no** form of this command to remove this router name and restore the default configuration.

Syntax

tunnel isatap router *router-name*

no tunnel isatap router

Parameters

router-name—Specifies the router's domain name.

Default Configuration

The automatic tunnel router's default domain name is ISATAP.

Command Mode

Interface Configuration (Tunnel) mode

User Guidelines

This command determines the string that the host uses for automatic tunnel router lookup in the IPv4 DNS procedure. By default, the string ISATAP is used for the corresponding automatic tunnel types.

Only one string can represent the automatic tunnel router name per tunnel. Using this command, therefore, overwrites the existing entry.

Example

The following example configures the global string ISATAP2 as the automatic tunnel router domain name.

```
switchxxxxxx(config)# tunnel 1
switchxxxxxx(config-tunnel)# tunnel isatap router ISATAP2
```

40.4 tunnel source

Use the **tunnel source** Interface Configuration (Tunnel) mode command to set the local (source) IPv4 address of a tunnel interface. The **no** form deletes the tunnel local address.

Syntax

tunnel source *{auto* | **ipv4-address** *ipv4-address}*

no tunnel source

Parameters

- **auto**—The system minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the IPv4 address is changed, then the local address of the tunnel interface is changed too.
- **ip4-address**—Specifies the IPv4 address to use as the source address for packets sent on the tunnel interface. The local address of the tunnel interface is not changed when the IPv4 address is moved to another interface (only if StackTable is changed).

Default

No source address is defined.

Command Mode

Interface Configuration (Tunnel) mode

User Guidelines

The configured source IPv4 address is used for forming the tunnel interface identifier. The interface identifier is set to the 8 least significant bytes of the SIP field of the encapsulated IPv6 tunneled packets.

Example

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-tunnel)# tunnel source auto
```

40.5 tunnel isatap query-interval

Use the **tunnel isatap query-interval** Global Configuration mode command to set the time interval between DNS queries (before the ISATAP router IP address is known) for the automatic tunnel router domain name. Use the **no** form of this command to restore the default configuration.

Syntax

tunnel isatap query-interval *seconds*

no tunnel isatap query-interval

Parameters

seconds—Specifies the time interval in seconds between DNS queries. (Range: 10–3600)

Default Configuration
The default time interval between DNS queries is 10 seconds.

Command Mode
Global Configuration mode

User Guidelines
This command determines the time interval between DNS queries before the ISATAP router IP address is known. If the IP address is known, the robustness level that is set by the tunnel isatap robustness Global Configuration mode command determines the refresh rate.

Example
The following example sets the time interval between DNS queries to 30 seconds.

```
switchxxxxxx(config)# tunnel isatap query-interval 30
```

40.6 tunnel isatap solicitation-interval
Use the **tunnel isatap solicitation-interval** Global Configuration mode command to set the time interval between ISATAP router solicitation messages. Use the **no** form of this command to restore the default configuration.

Syntax
tunnel isatap solicitation-interval *seconds*

no tunnel isatap solicitation-interval

Parameters
seconds—Specifies the time interval in seconds between ISATAP router solicitation messages. (Range: 10–3600)

Default Configuration
The default time interval between ISATAP router solicitation messages is 10 seconds.

Command Mode
Global Configuration mode

User Guidelines
This command determines the interval between router solicitation messages when there is no active ISATAP router. If there is an active ISATAP router, the robustness level set by the **tunnel isatap robustness** Global Configuration mode command determines the refresh rate.

Example
The following example sets the time interval between ISATAP router solicitation messages to 30 seconds.

```
switchxxxxxx(config)# tunnel isatap solicitation-interval 30
```

40.7 tunnel isatap robustness

Use the **tunnel isatap robustness** Global Configuration mode command to configure the number of DNS query/router solicitation refresh messages that the device sends. Use the **no** form of this command to restore the default configuration.

Syntax

tunnel isatap robustness *number*

no tunnel isatap robustness

Parameters

number—Specifies the number of DNS query/router solicitation refresh messages that the device sends. (Range: 1–20)

Default Configuration

The default number of DNS query/router solicitation refresh messages that the device sends is 3.

Command Mode

Global Configuration mode

User Guidelines

The DNS query interval (after the ISATAP router IP address is known) is the Time-To-Live (TTL) that is received from the DNS, divided by (Robustness + 1).

The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router, divided by (Robustness + 1).

Example

The following example sets the number of DNS query/router solicitation refresh messages that the device sends to 5.

```
switchxxxxxx(config)# tunnel isatap robustness 5
```

40.8 show ipv6 tunnel

Use the **show ïpv6 tunnel** EXEC mode command to display information on the ISATAP tunnel.

Syntax

show ïpv6 tunnel

Command Mode

EXEC mode

Example

The following example displays information on the ISATAP tunnel.

```
switchxxxxxx#  show ipv6 tunnel
```

```
Tunnel 1
--------
Tunnel status                    : DOWN
Tunnel protocol                  : NONE
Tunnel Local address type        : auto
Tunnel Local Ipv4 address        : 0.0.0.0
Router DNS name                  : ISATAP
Router IPv4 address              : 0.0.0.0
DNS Query interval               : 300 seconds
Min DNS Query interval           : 0 seconds
Router Solicitation interval     : 10 seconds
Min Router Solicitation interval : 0 seconds
Robustness                       : 2
```

41 DHCP Relay Commands

41.1 ip dhcp relay enable (Global)

Use the **ip dhcp relay enable** Global Configuration mode command to enable the DHCP relay feature on the device. Use the **no** form of this command to disable the DHCP relay feature.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Parameters

N/A

Default Configuration

DHCP relay feature is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP relay feature on the device.

```
switchxxxxxx(config)# ip dhcp relay enable
```

41.2 ip dhcp relay enable (Interface)

Use the **ip dhcp relay enable** Interface Configuration (VLAN, Ethernet, Port-channel) mode command to enable the DHCP relay feature on an interface. Use the **no** form of this command to disable the DHCP relay agent feature on an interface.

Syntax

ip dhcp relay enable

no ip dhcp relay enable

Parameters

N/A

Default Configuration

Disabled

Command Mode

Interface Configuration (VLAN, Ethernet, Port-channel) mode

User Guidelines

The operational status of DHCP Relay on an interface is active if one of the following conditions exist:

- DHCP Relay is globally enabled, and there is an IP address defined on the interface.
  Or
- DHCP Relay is globally enabled, there is no IP address defined on the interface, the interface is a VLAN, and option 82 is enabled.

Example

The following example enables DHCP Relay on VLAN 21.

```
switchxxxxxx(config)# interface vlan 21
switchxxxxxx(config-if)# ip dhcp relay enable
```

41.3 ip dhcp relay address

Use the **ip dhcp relay address** Global Configuration mode command to define the DHCP servers available for the DHCP relay. Use the **no** form of this command to remove servers from the list.

Syntax

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Parameters

ip-address—Specifies the DHCP server IP address. Up to 8 servers can be defined.

Default Configuration

No server is defined.

Command Mode

Global Configuration mode

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

41.4 show ip dhcp relay

Use the **show ip dhcp relay** EXEC mode command to display the DHCP relay information.

Syntax

show ip dhcp relay

Command Mode

EXEC mode

Example

Example 1. Option 82 is not supported:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is Disabled
Maximum number of supported VLANs without IP Address is 256
Number of DHCP Relays enabled on VLANs without IP Address is 0
DHCP relay is not configured on any port.
DHCP relay is not configured on any vlan.
No servers configured
```

Example 2. Option 82 is supported (disabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: fe1/0/15,po3-4
 Active:
 Inactive: fe1/0/15, po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active:
 Inactive: 1, 2, 4, 5
Servers: 1.1.1.1 , 2.2.2.2
```

Example 3. Option 82 is supported (enabled):

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: fe1/0/15,po3-4
 Active: fe1/0/15
 Inactive: po3-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active: 1, 2, 4, 5
 Inactive:
Servers: 1.1.1.1 , 2.2.2.2
```

41.5 ip dhcp information option

Use the **ip dhcp information option** Global Configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

Syntax

ip dhcp information option

no ip dhcp information option

Parameters

N/A

Default Configuration

DHCP option-82 data insertion is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP option 82 would be enabled only if DHCP snooping or DHCP relay are enabled.

Example

```
switchxxxxxx(config)# ip dhcp information option
```

41.6 show ip dhcp information option

The **show ip dhcp information option** EXEC mode command displays the DHCP Option 82 configuration.

Syntax

show ip dhcp information option

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

Example

The following example displays the DHCP Option 82 configuration.

```
switchxxxxxx# show ip dhcp information option
```

```
Relay agent Information option is Enabled
```

42 DHCP Server Commands

42.1 ip dhcp server

Use the **ip dhcp server** Global Configuration mode command to enable the Dynamic Host Configuration Protocol (DHCP) server features on the device. Use the **no** form of this command to disable the DHCP server.

Syntax

ip dhcp server

no ip dhcp server

Default Configuration

The DHCP server is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the DHCP server on the device:

```
Console(config)# ip dhcp server
```

42.2 ip dhcp pool host

Use the **ip dhcp pool host** Global Configuration mode command to configure a Dynamic Host Configuration Protocol (DHCP) static address on a DHCP Server and enter the DHCP Pool Host Configuration mode. Use the **no** form of this command to remove the address pool.

Syntax

ip dhcp pool host *name*

no ip dhcp pool host *name*

Parameters

name—Specifies the DHCP address pool name. It can be either a symbolic string (such as Engineering) or an integer (such as 8). (Length: 1–32 characters)

Default Configuration

DHCP hosts are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to the DHCP Pool Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure host parameters, such as the IP subnet number and default router list.

Example

The following example configures Station as the DHCP address pool:

```
Console(config)# ip dhcp pool host station
Console(config-dhcp)#
```

42.3 ip dhcp pool network

Use the **ip dhcp pool network** Global Configuration mode command to configure a Dynamic Host Configuration Protocol (DHCP) address pool on a DHCP Server and enter DHCP Pool Configuration mode. Use the **no** form of this command to remove the address pool.

Syntax

ip dhcp pool network *name*

no ip dhcp pool network *name*

Parameters

name—Specifies the DHCP address pool name. It can be either a symbolic string (such as ‘engineering’) or an integer (such as 8). (Length: 1–32 characters)

Default Configuration

DHCP address pools are not configured.

Command Mode

Global Configuration mode

User Guidelines

During execution of this command, the configuration mode changes to DHCP Pool Network Configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Example

The following example configures Pool1 as the DHCP address pool.

```
Console(config)# ip dhcp pool network pool1
Console(config-dhcp)#
```

42.4 address (DHCP Host)

Use the **address** DHCP Pool Host Configuration mode command to manually bind an IP address to a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the IP address binding to the client.

Syntax

address *ip-address* {*mask* | *prefix-length*} *{client-identifier unique-identifier | hardware-address mac-address}*

no address

Parameters

- **address**—Specifies the client IP address.
- **mask**—Specifies the client network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **unique-identifier**—Specifies the distinct client identification in dotted hexadecimal notation: Each byte in a hexadecimal character string is two hexadecimal digits. Bytes are separated by a period or colon. For example, 01b7.0813.8811.66.
- **hardware-address**—Specifies the MAC address.

Default Configuration

DHCP hosts are not configured.

Command Mode

DHCP Pool Host Configuration mode

Example

The following example manually binds an IP address to a Dynamic Host Configuration Protocol (DHCP) client.

```
Console(config-dhcp)# address 10.12.1.99 255.255.255.0 01b7.0813.8811.66
```

42.5 address (DHCP Network)

Use the **address** DHCP Pool Network Configuration mode command to configure the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on DHCP Server. Use the **no** form of this command to remove the subnet number and mask.

Syntax

address *{network-number | low low-address high high-address} {mask | prefix-length}*
no address

Parameters

- **network-number**—Specifies the IP address of the DHCP address pool.
- **mask**—Specifies the pool network mask.
- **prefix-length**—Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the client network mask. The prefix length must be preceded by a forward slash (/).
- **low** *low-address*—Specifies the first IP address to use in the address range.
- **high high-address**—Specifies the last IP address to use in the address range.

Default Configuration
DHCP address pools are not configured.

If the low address is not specified, it defaults to the first IP address in the network.

If the high address is not specified, it defaults to the last IP address in the network.

Command Mode
DHCP Pool Network Configuration mode

Example
The following example configures the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on DHCP Server.

```
Console(config-dhcp)# address 10.12.1.0 255.255.255.0
```

42.6 lease
Use the **lease** DHCP Pool Network Configuration mode command to configure the time duration of the lease for an IP address that is assigned from a Dynamic Host Configuration Protocol (DHCP) Server to a DHCP client. Use the **no** form of this command to restore the default value.

Syntax
lease {*days* [{*hours*} [*minutes*]*]* | *infinite}*

no lease

Parameters
- **days**—Specifies the number of days in the lease.
- **hours**—Specifies the number of hours in the lease. A **days** value must be supplied before configuring an ***hours*** value.
- **minutes**—Specifies the number of minutes in the lease. A **days** value and an **hours** value must be supplied before configuring a **minutes** value.
- **infinite**—Specifies that the duration of the lease is unlimited.

Default Configuration
The default lease duration is 1 day.

Command Mode
DHCP Pool Network Configuration mode

Examples
The following example shows a 1-day lease.

```
Console(config-dhcp)# lease 1
```

The following example shows a one-hour lease.

```
Console(config-dhcp)# lease 0 1
```

The following example shows a one-minute lease.

```
Console(config-dhcp)# lease 0 0 1
```

The following example shows an infinite (unlimited) lease.

```
Console(config-dhcp)# lease infinite
```

42.7 client-name

Use the **client-name** DHCP Pool Host Configuration mode command to define the name of a DHCP client. The client name should not include the domain name. Use the **no** form of this command to remove the client name.

Syntax

client-name *name*

no client-name

Parameters

name—Specifies the client name, using standard ASCII characters. The client name should not include the domain name. For example, the name Mars should not be specified as mars.yahoo.com. (Length: 1–32 characters)

Command Mode

DHCP Pool Host Configuration mode

Default Coniguration

No client name is defined.

Example

The following example defines the string Client1 as the client name.

```
Console(config-dhcp)# client-name client1
```

42.8 default-router

Use the **default-router** DHCP Pool Configuration mode command to configure the default router list for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the default router list.

Syntax

default-router *ip-address* [*ip-address2 ... ip-address8*]

no default-router

Parameters
ip-address—Specifies the IP address of a router. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No default router is defined.

User Guidelines
The router IP address should be on the same subnet as the client subnet.

Example
The following example specifies 10.12.1.99 as the default router IP address.

```
Console(config-dhcp)# default-router 10.12.1.99
```

42.9 dns-server
Use the **dns-server** DHCP Pool Configuration mode command to configure the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the DNS server list.

Syntax
dns-server *ip-address* [*ip-address2* ... *ip-address8*]

no dns-server

Parameters
ip-address—Specifies a DNS Server IP address. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No DNS server is defined.

User Guidelines
If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Example
The following example specifies 10.12.1.99 as the client domain name server IP address.

```
Console(config-dhcp)# dns-server 10.12.1.99
```

42.10 domain-name
Use the **domain-name** DHCP Pool Configuration mode command to specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the domain name.

Syntax
domain-name *domain*

no domain-name

Parameters
domain—Specifies the DHCP client domain name string. (Length: 1–32 characters)

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No domain name is defined.

Example
The following example specifies yahoo.com as the DHCP client domain name string.

```
Console(config-dhcp)# domain-name yahoo.com
```

42.11 netbios-name-server
Use the **netbios-name-server** DHCP Pool Configuration mode command to configure the NetBIOS Windows Internet Naming Service (WINS) servers that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the **no** form of this command to remove the NetBIOS name server list.

Syntax
netbios-name-server *ip-address* [*ip-address2 ... ip-address8*]

no netbios-name-server

Parameters
ip-address—Specifies the NetBIOS WINS name server IP address. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
No bios server is defined.

Example
The following example specifies the IP address of a NetBIOS name server available to the DHCP client.

```
Console(config-dhcp)# netbios-name-server 10.12.1.90
```

42.12 netbios-node-type
Use the **netbios-node-type** DHCP Pool Configuration mode command to configure the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the **no** form of this command to return to default.

Syntax
netbios-node-type {**b-node** | **p-node** | **m-node** | **h-node**}

no netbios-node-type

Parameters
- **b-node**—Specifies the Broadcast NetBIOS node type.
- **p-node**—Specifies the Peer-to-peer NetBIOS node type.
- **m-node**—Specifies the Mixed NetBIOS node type.
- **h-node**—Specifies the Hybrid NetBIOS node type.

Command Mode
DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration
h-node (Hybrid NetBIOS node type).

Example
The following example specifies the client's NetBIOS type as mixed.

```
Console(config-dhcp)# netbios node-type m-node
```

42.13 next-server
Use the **next-server** DHCP Pool Configuration mode command to configure the next server in the boot process of a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the boot server.

Syntax

next-server *ip-address*

no next-server

Parameters

ip-address—Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Configuration

If the **next-server** command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Example

The following example specifies 10.12.1.99 as the IP address of the next server in the boot process.

```
Console(config-dhcp)# next-server 10.12.1.99
```

42.14 next-server-name

Use the **next-server-name** DHCP Pool Configuration mode command to configure the next server name in the boot process of a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the boot server name.

Syntax

next-server-name *name*

no next-server-name

Parameters

name—Specifies the name of the next server in the boot process. (Length: 1–64 characters)

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration

No next server name is defined.

Example

The following example specifies www.bootserver.com as the name of the next server in the boot process of a DHCP client.

```
Console(config-dhcp)# next-server www.bootserver.com
```

42.15 bootfile

Use the **bootfile** DHCP Pool Configuration mode command to specify the default boot image file name for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to delete the boot image file name.

Syntax

bootfile *filename*

no bootfile

Parameters

filename—Specifies the file name used as a boot image. (Length: 1–128 characters)

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Example

The following example specifies boot_image_file as the default boot image file name for a DHCP client.

```
Console(config-dhcp)# bootfile boot_image_file
```

42.16 time-server

Use the **time-server** DHCP Pool Configuration mode command to specify the time servers list for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the time servers list.

Syntax

time-server *ip-address* [*ip-address2 ... ip-address8*]

no time-server

Parameters

ip-address—Specifies the IP address of a time server. One IP address is required, although up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

Default Configuration

No time server name is defined.

User Guidelines

The router IP address should be on the same subnet as the client subnet.

Example

The following example specifies 10.12.1.99 as the time server IP address.

```
Console(config-dhcp)# time-server 10.12.1.99
```

42.17 option

Use the **option** DHCP Pool Configuration mode command to configure the Dynamic Host Configuration Protocol (DHCP) Server options. Use the **no** form of this command to remove the options.

Syntax

option *code {ascii ascii-string | hex hex-string | ip ip-address}*

option ip-list *code ip-address1* [*ip-address2* …]

no option *code*

Parameters

- **code**—Specifies the DHCP option code.
- **ascii ascii-string**—Specifies an NVT ASCII character string. ASCII character strings, which contain white space, must be delimited by quotation marks.
- **hex hex-string**—Specifies dotted hexadecimal data: Each byte in hexadecimal character strings is two hexadecimal digits. Bytes are separated by a period or colon.
- **ip ip-address**—Specifies an IP address.
- **ip-list**—Specifies that a list of IP addresses immediately follows the option code.
- ***ip-address1* [*ip-address2* …]**—Specifies a list of one or more IP addresses.

Command Mode

DHCP Pool Host Configuration mode

DHCP Pool Network Configuration mode

User Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the DHCP message options field. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, *Dynamic Host Configuration Protocol*.

For options in hexadecimal format, the string parameter should include all the bytes in the option value, including leading zeros.

Examples

The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable Ip forwarding. A value of 1 means enable IP forwarding. IP forwarding is enabled in the following example.

```
Console(config-dhcp)# option 19 hex 01
```

The following example configures DHCP option 2, which specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). A value of 0xE10 in the following example indicates a location 1 hour east of the meridian.

```
Console(config-dhcp)# option 2 hex 00000E10
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example.

```
Console(config-dhcp)# option ip-list 72 172.16.3.252 172.16.3.253
```

42.18 ip dhcp excluded-address

Use the **ip dhcp excluded-address** Global Configuration mode command to specify the IP addresses that a Dynamic Host Configuration Protocol (DHCP) Server should not assign to DHCP clients. Use the **no** form of this command to remove the excluded IP addresses.

Syntax

ip dhcp excluded-address *low-address* [*high-address*]

no ip dhcp excluded-address *low-address* [*high-address*]

Parameters

- **low-address**—Specifies the excluded IP address, or first IP address in an excluded address range.
- **high-address**—Specifies the last IP address in the excluded address range.

Default Configuration

All IP pool addresses are assignable.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Server assumes that all pool addresses can be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Example

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199.

```
Console(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

42.19 ip dhcp ping enable

Use the **ip dhcp ping enable** Global Configuration mode command to enable the Dynamic Host Configuration Protocol (DHCP) Server to send ping packets before assigning the address to a

requesting client. Use the **no** form of this command to prevent the server from pinging pool addresses.

Syntax
ip dhcp ping enable

no ip dhcp ping enable

Default Configuration
DHCP pinging is disabled.

Command Mode
Global Configuration mode

User Guidelines
The DHCP Server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP Server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Example
The following example enables the DHCP Server to send ping packets before assigning the address to a requesting client.

```
Console(config)# ip dhcp ping enable
```

42.20 ping enable
Use the **ping enable** DHCP Pool Network Configuration mode command to enable the Dynamic Host Configuration Protocol (DHCP) Server to send ping packets before assigning the address to a requesting client. Use the **no** form of this command to prevent the server from pinging pool addresses.

Syntax
ping enable

no ping enable

Default Configuration
The default configuration is set to enable.

Command Mode
DHCP Pool Network Configuration mode

User Guidelines
The DHCP Server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP Server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Example
The following example enables the DHCP Server to send ping packets before assigning the address to a requesting client.

```
Console(config-dhcp)# ping enable
```

42.21 ip dhcp ping count
Use the **ip dhcp ping count** Global Configuration mode command to specify the number of packets a Dynamic Host Configuration Protocol (DHCP) Server sends to a pool address as part of a ping operation. Use the **no** form of this command to restore the default configuration.

Syntax
ip dhcp ping count *number*

no ip dhcp ping count

Parameters
number—Specifies the number of ping packets that are sent before assigning the address to a requesting client. (Range: 1-10)

Default Configuration
A Dynamic Host Configuration Protocol (DHCP) Server sends two packets to a pool address as part of a ping operation.

Command Mode
Global Configuration mode

Example
The following example specifies that a DHCP Server sends five packets to a pool address as part of a ping operation.

```
Console(config)# ip dhcp ping count 5
```

42.22 ip dhcp ping timeout
The **ip dhcp ping timeout** Global Configuration mode command specifies the time interval during which a Dynamic Host Configuration Protocol (DHCP) Server waits for a ping reply from an address pool. To restore the default timeout, use the **no** form of this command.

Syntax
ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Parameters
milliseconds — Specifies the amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The timeout range is 300-10000 milliseconds.

Default Configuration
The default timeout is 500 milliseconds.

Command Mode
Global Configuration mode

User Guidelines
This command specifies how long to wait for a ping reply (in milliseconds).

Example
The following example specifies that a DHCP Server waits 1 second for a ping reply from an address pool before it stops attempting to reach a pool address for client assignment.

```
Console(config)# ip dhcp ping timeout 1000
```

42.23 clear ip dhcp binding
The **clear ip dhcp binding** Privileged EXEC mode command deletes the dynamic address binding from the Dynamic Host Configuration Protocol (DHCP) Server database.

Syntax
clear ip dhcp binding {*address* | ***}

Parameters
- *address* — Specifies the binding address to delete from the DHCP database.
- * — Clears all automatic bindings.

Command Mode
Privileged EXEC mode

User Guidelines
Typically, the address denotes the client IP address. If the asterisk (*) character is specified as the address parameter, DHCP clears all dynamic bindings.

Use the **no ip dhcp pool** Global Configuration mode command to delete a manual binding.

Example
The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Console# clear ip dhcp binding 10.12.1.99
```

42.24 show ip dhcp
The **show ip dhcp** EXEC mode command displays the DHCP configuration.

Syntax
show ip dhcp

Command Mode
EXEC mode

Example
The following example displays the DHCP configuration.

```
console#  show ip dhcp

DHCP server is enabled.
DHCP ping packets is enabled with 2 retries and 500 milliseconds.
```

42.25 show ip dhcp excluded-addresses
The **show ip dhcp excluded-addresses** EXEC mode command displays the excluded addresses.

Syntax
show ip dhcp excluded-addresses

Command Mode
EXEC mode

Example
The following example displays the excluded addresses.

```
console#  show ip dhcp excluded-addresses
The number of excluded addresses ranges is 2
Excluded addresses:
10.1.1.212- 10.1.1.219, 10.1.2.212- 10.1.2.219
```

42.26 show ip dhcp pool host
The **show ip dhcp pool host** EXEC mode command displays the DHCP pool host configuration.

Syntax
show ip dhcp pool host [*address* | *name*]

Parameters
- *address* — Specifies the client IP address.
- *name* — Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode
EXEC mode

Example

The following example displays the DHCP pool host configuration.

```
console#  show ip dhcp pool host
The number of host pools is 1


Name          IP Address       Hardware      Client Identifier
---------     --------------   Address       --------------
Station       172.16.1.11      ----------    01b7.0813.8811.66

console#  show ip dhcp pool host station

Name          IP Address       Hardware      Client Identifier
---------     --------------   Address       --------------
Station       172.16.1.11      ----------    01b7.0813.8811.66

Mask: 255.255.0.0
Default router: 172.16.1.1
Client name: client1
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code          Value
----          -----
19            Ox01
```

42.27 show ip dhcp pool network

The **show ip dhcp pool network** EXEC mode command displays the DHCP network configuration.

Syntax

show ip dhcp pool network [*name*]

Parameters

name — Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

EXEC mode

Example

```
Router> show ip dhcp pool network
```

```
The number of network pools is 2
Name Address range mask Lease
-------------------------------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
finance 10.1.2.8-10.1.2.178 255.255.255.0 0d:12h:0m
Router> show ip dhcp pool network marketing
Name Address range mask Lease
--------------------------------- ------------------------
marketing 10.1.1.17-10.1.1.178 255.255.255.0 0d:12h:0m
Statistics:
All-range Available Free Pre-allocated Allocated Expired   Declined
---------- ---------   ----- -------------   --------- --------- --------
162 150 68 50 20        3         9
Default router: 10.1.1.1
Ping packets: enabled
DNS server: 10.12.1.99
Domain name: yahoo.com
NetBIOS name server: 10.12.1.90
NetBIOS node type: h-node
Next server: 10.12.1.99
Next-server-name: 10.12.1.100
Bootfile: Bootfile
Time server 10.12.1.99
Options:
Code Value
------------------
19 Ox01
```

42.28 show ip dhcp binding

Use the **show ip dhcp binding** EXEC mode command to display the specific one or all the address bindings on the Dynamic Host Configuration Protocol (DHCP) Server.

Syntax

show ip dhcp binding [*ip-address***]**

Parameters

ip-address — Specifies the IP address

Command Mode

EXEC mode

Example

The following example displays the DHCP Server binding address parameters.

```
Router> show ip dhcp binding
```

```
DHCP server enabled
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1

IP address Hardware Address Lease Expiration Type    State
---------- ---------------- -------------    ------- ---------
1.16.1.11  00a0.9802.32de    Feb 01 1998     dynamic allocated
1.16.3.23  02c7.f801.0422    12:00AM         dynamic expired
1.16.3.24  02c7.f802.0422                    dynamic declined
1.16.3.25  02c7.f803.0422                    dynamic pre-allocated
1.16.3.26  02c7.f804.0422                    dynamic declined

Router> show ip dhcp binding 1.16.1.11
DHCP server enabled
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1

IP address Hardware Address Lease Expiration  Type    State
---------- ---------------- ----------------- ------- ---------
1.16.1.11  00a0.9802.32de    Feb 01 1998      dynamic allocated
                            12:00 AM

Router> show ip dhcp binding 1.16.3.24
The number of used (all types) entries is 6
The number of pre-allocated entries is 1
The number of allocated entries is 1
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1

IP address Hardware Address Lease Expiration   Type    State
```

```
---------- ----------------   ---------------  ------- ---------
1.16.3.24  02c7.f802.0422                     dynamic declined
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.
State	The IP Address state.

42.29 show ip dhcp server statistics

Use the **show ip dhcp server statistics** EXEC command to display Dynamic Host Configuration Protocol (DHCP) Server statistics.

Syntax

show ip dhcp server statistics

Command Mode

EXEC mode

Example

The following example displays DHCP Server statistics

```
DHCP server enabled
The number of network pools is 7
The number of excluded pools is 2
The number of used (all types) entries is 7
The number of pre-allocated entries is 1
The number of allocated entries is 3
The number of expired entries is 1
The number of declined entries is 2
The number of static entries is 1
The number of dynamic entries is 2
The number of automatic entries is 1
```

42.30 show ip dhcp allocated

Use the **show ip dhcp allocated** EXEC mode command to display the specific one or all the allocated address on the Dynamic Host Configuration Protocol (DHCP) Server.

Syntax
show ip dhcp allocated *[ip-address]*

Parameters
ip-address — Specifies the IP address

Command Mode
EXEC mode

Example
The following example displays the DHCP Server allocated IP addresses.

```
Router> show ip dhcp allocated
DHCP server enabled
The number of allocated entries is 3

IP address   Hardware address Lease expiration      Type
----------   ---------------- --------------------  ---------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic
172.16.3.253 02c7.f800.0422   Infinite              Automatic
172.16.3.254 02c7.f800.0422   Infinite              Static

Router> show ip dhcp allocated 172.16.1.11
DHCP server enabled
The number of allocated entries is 2

IP address   Hardware address Lease expiration      Type
----------   ---------------- --------------------  --------
172.16.1.11  00a0.9802.32de   Feb 01 1998 12:00 AM  Dynamic

Router> show ip dhcp allocated 172.16.3.254
DHCP server enabled
The number of allocated entries is 2

IP address   Hardware address Lease expiration      Type
----------   ---------------- --------------------  -------
172.16.3.254 02c7.f800.0422   Infinite              Static
```

The following table describes the significant fields shown in the display.

Field	Description
IP address	The host IP address as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.

Lease expiration	The lease expiration date of the host IP address.
Type	The manner in which the IP address was assigned to the host.

42.31 show ip dhcp declined

Use the **show ip dhcp declined** EXEC command to display the specific one or all the declined addresses on the Dynamic Host Configuration Protocol (DHCP) server.

show ip dhcp declined Field Descriptions

Syntax

show ip dhcp declined *[ip-address]*

Parameters

ip-address—Specifies the IP address.

Command Mode

EXEC mode

Example

```
Router> show ip dhcp declined
DHCP server enabled
The number of declined entries is 2

IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422

Router> show ip dhcp declined 172.16.1.11
DHCP server enabled
The number of declined entries is 2

IP address    Hardware address
172.16.1.11   00a0.9802.32de
```

42.32 show ip dhcp expired

Use the **show ip dhcp expired** EXEC command to display the specific one or all the expired addresses on the Dynamic Host Configuration Protocol (DHCP) server.

Syntax

show ip dhcp expired *[ip-address]*

Parameters

ip-address—Specifies the IP.

Command Mode
EXEC mode

Example

```
Router> show ip dhcp expired
DHCP server enabled
The number of expired entries is 1

IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422

Router> show ip dhcp expired 172.16.1.11
DHCP server enabled
The number of expired entries is 1

IP address  Hardware address
172.16.1.13 00a0.9802.32de
```

42.33 show ip dhcp pre-allocated

Use the **show ip dhcp pre-allocated** EXEC command to display the specific one or all the pre-allocated addresses on the Dynamic Host Configuration Protocol (DHCP) server.

Syntax
show ip dhcp pre-allocated *[ip-address]*

Parameters
ip-address—Specifies the IP.

Command Mode
EXEC mode

Examples

```
Router> show ip dhcp pre-allocated
DHCP server enabled
The number of pre-allocated entries is 1

IP address   Hardware address
172.16.1.11  00a0.9802.32de
172.16.3.254 02c7.f800.0422

Router> show ip dhcp pre-allocated 172.16.1.11
DHCP server enabled
```

```
The number of pre-allocated entries is 1

IP address   Hardware address
172.16.1.15  00a0.9802.32de
```

43 IP Routing Protocol-Independent Commands

43.1 ip route

Use the **ip route** Global Configuration mode command to configure static routes. Use the **no** form of this command to remove static routes.

Syntax

ip route *prefix* {*mask* | *prefix-length*} {{*ip-address* [**metric** *distance*]} | **reject-route**}

no ip route *prefix* {*mask* | *prefix-length*} [*ip-address*]

Parameters

- **prefix**—Specifies the IP address that is the IP route prefix for the destination IP.
- **mask**—Specifies the network subnet mask of the IP address prefix.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- **ip-address**—Specifies the IP address or IP alias of the next hop that can be used to reach the network.
- **metric** *distance*—Specifies an administrative distance. (Range: 1–255).
- **reject-route**—Stops routing to the destination network via all gateways.

Default Configuration

The default administrative distance is 1.

Command Mode

Global Configuration mode

User Guidelines

Use the **no ip route** command with the *ip-address* parameter to remove a single static route to the given subnet via the given next hop.

Use the **no ip route** command without the i*p-address* parameter to remove all static routes to the given subnet.

Examples

Example 1 - The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
switchxxxxxx(conf)#ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

Example 2 - The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length:

```
switchxxxxxx(conf)#ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

Example 3 - The following example shows how to reject packets for network 194.1.1.0:

```
switchxxxxxx(conf)#ip route 194.1.1.0 255.255.255.0 reject-route
```

Example 4 - The following example shows how to remove all static routes to network 194.1.1.0/24:

```
switchxxxxxx(conf)#no ip route 194.1.1.0 /24
```

Example 5 - The following example shows how to remove one static route to network 194.1.1.0/24 via 1.1.1.1:

```
switchxxxxxx(conf)#no ip route 194.1.1.0 /24 1.1.1.1
```

43.2 ip routing

Use the **ip routing** Global Configuration mode command to enable IPv4 Routing. Use the **no** format of the command to disable IPv4 Routing.

Syntax

ip routing

no ip routing

Parameters

N/A

Default Configuration

Enabled.

Command Mode

Global Configuration mode

Example. The following example enables ipv4 routing.

```
switchxxxxxx# ip routing
```

43.3 key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the **key chain** command in Global Configuration mode. This command puts the user into the Keychain mode.

To remove the key chain, use the **no** form of this command.

Syntax

key chain *name-of-chain*

no key chain *chain-name*

Parameters

name-of-chain—Name of a key chain. The chain-name may have from 1 to 32 characters. A key chain must have at least one key and can have up to 256 keys.

Default Configuration

No key chain exists.

Command Mode

Global Configuration mode

User Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, it is recommended to use a single key chain per interface per routing protocol. The **key chain** command enters the **key-chain** configuration mode.

Example

The following example configures a key chain named chain1. The key named **key1** will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named **key2** will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(conf)#key chain chain1
switchxxxxxx(config-keychain)#key 1
switchxxxxxx(config-keychain-key)key-string key1
switchxxxxxx(config-keychain-key)accept-lifetime 13:30:00 Jan 25 2011
duration 7200
switchxxxxxx(config-keychain-key)send-lifetime 14:00:00 Jan 25 2011
duration 3600
switchxxxxxx(config-keychain-key)key 2
switchxxxxxx(config-keychain-key)key-string key2
switchxxxxxx(config-keychain-key)accept-lifetime 14:30:00 Jan 25 2011
duration 7200
switchxxxxxx(config-keychain-key)send-lifetime 15:00:00 Jan 25 2011
duration 3600
switchxxxxxx(config-keychain-key)#exit
switchxxxxxx(config-keychain)#exit
switchxxxxxx(config)#exit
switchxxxxxx(config)#router rip
switchxxxxxx(config-router-rip)#network 172.19.1.1
switchxxxxxx(config-router-rip)#exit
switchxxxxxx(config)interface ip 172.19.1.1
switchxxxxxx(config)ip rip authentication mode md5
switchxxxxxx(config-interface)#ip rip authentication key-chain chain1
switchxxxxxx(config-interface)#exit
```

43.4 key (key chain)

Use the **key** command in Key-chain Configuration mode to identify an authentication key on a key chain. This command places the user in Keychain Key mode.

To remove the key from the key chain, use the **no** form of this command.

Syntax

key *key-id*

no key *key-id*

Parameters

key-id—Identification number of an authentication key on a key chain. The range of keys is from 1 to 255. The key identification numbers need not be consecutive. The scope of a key identification number is the key chain where the key is defined.

Default Configuration

No key exists on the key chain.

Command Mode

Key-Chain Configuration mode

User Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the accept-lifetime and send-lifetime key chain key command settings.

Each key has its own key identifier that is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will be finished with an error.

To remove all keys, remove the key chain by using the **no key chain** command.

Example

The following example configures a key chain named **chain1**. The key named **key**1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named **key2** will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key 1
key chain chain1
 key 1
 key-string key1
 accept-lifetime 13:30:00 Jan 25 2011 duration 7200
 send-lifetime 14:00:00 Jan 25 2011 duration 3600
 key 2
 key-string key2
```

```
 accept-lifetime 14:30:00 Jan 25 2011 duration 7200
 send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit
router rip
 network 172.19.1.1
exit
interface ip 172.19.1.1
 ip rip authentication mode md5
 ip rip authentication key-chain chain1
exit
```

43.5 key-string

To specify the authentication string for a key, use the **key-string** command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

Syntax

key-string *text*

no key-string

Parameters

text—Specifies the authentication string. The string can contain from 1 to 16 characters.

Default Configuration

N/A

Command Mode

Key chain key configuration.

Example

The following example configures a key chain named **chain1**. The key named **key1** will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named **key2** will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
key chain chain1
 key 1
 key-string key1
 accept-lifetime 13:30:00 Jan 25 2011 duration 7200
 send-lifetime 14:00:00 Jan 25 2011 duration 3600
 key 2
 key-string key2
 accept-lifetime 14:30:00 Jan 25 2011 duration 7200
 send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit
```

```
router rip
 network 172.19.1.1
 version 2
exit
interface ip 172.19.1.1
 ip rip authentication key-chain chain1
 ip rip authentication mode md5
exit
```

43.6 accept-lifetime

Use the **accept-lifetime** command in Key Chain Key Configuration mode to set the time period during which the authentication key on a key chain is received as valid. To revert to the default value, use the **no** form of this command.

Syntax

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime

Parameters

- **start-time**—Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following:
  - *hh*:*mm*:*ss month day year*
  - *hh*:*mm*:*ss day month year*
  - *hh*—hours (0-23)
  - *mm*—minutes (0-59
  - *ss*—seconds (0-59)
  - *month*—first three letters of the month
  - *day*—day (1-31)
  - *year*—year (four digits)
- **infinite**—Key is valid to be received from the *start-time* value on.
- **end-time**—Key is valid to be received from the *start-time* value until the *end-time value*. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
- **duration** *seconds*—Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Default Configuration

The default start time and the earliest acceptable date is January 1, 2000.

The default time period during which the authentication key is valid for authenticating incoming packets is set to forever and the ending time is infinite.

Command Mode

Key chain key configuration

User Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

A key is considered as expired if Time-of-Date is not set by management or by SNTP.

If the last key expires, authentication will be finished with error.

Example

The following example configures a key chain called **keychain1**. The key named **string1** will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named **string2** will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
router rip
 network 172.19.1.1
exit
interface ip 172.19.1.1
 ip rip authentication mode md5
 ip rip authentication key-chain keychain1
exit
key chain keychain1
 key 1
 key-string string1
 accept-lifetime 13:30:00 Jan 25 2011 duration 7200
 send-lifetime 14:00:00 Jan 25 2011 duration 3600
 key 2
 key-string string2
 accept-lifetime 14:30:00 Jan 25 2011 duration 7200
 send-lifetime 15:00:00 Jan 25 2011 duration 3600
exit
```

43.7 send-lifetime

Use the **send-lifetime** command in Key Chain Key Configuration mode to set the time period during which an authentication key on a key chain is valid to be sent. To revert to the default value, use the **no** form of this command.

Syntax

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

Parameters

- **start-time**—Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following:
  - *hh*:*mm*:*ss month day year*
  - *hh*:*mm*:*ss day month year*
  - *hh*—hours (0-23)
  - *mm*—minutes (0-59
  - *ss*—seconds (0-59)

  - *month*—first three letters of the month
  - *day*—day (1-31)
  - *year*—year (four digits)
- **infinite**—Key is valid to be received from the *start-time* value on.
- **end-time**—Key is valid to be received from the *start-time* value until the *end-time value*. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
- **duration** *seconds*—Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Default Configuration

The default start time and the earliest acceptable date is January 1, 2000.

The default time period during which the authentication key is valid for authenticating incoming packets is set to forever and the ending time is infinite.

Command Mode

Key chain key configuration

User Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

A key is considered as expired if Time-of-Date is not set by management or by SNTP.

If the last key expires, authentication will be finished with error.

Example

The following example configures a key chain called **chain1**. The key named **key1** will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named **key2** will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
router rip
 network 172.19.1.1
exit
interface ip 172.19.1.1
 ip rip authentication mode md5
 ip rip authentication key-chain chain1
exit
key chain chain1
 key 1
 key-string key1
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string key2
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

```
exit
```

43.8 show ip route

Use the **show ip route** EXEC mode command to display the current routing table state.

Syntax

show ip route *[connected | static | {**address** address [mask | prefix-length] **[longer-prefixes]**}]*

Parameters

- **connected**—Displays connected routing entries only.
- **static**—Displays static routing entries only.
- **address address**—Specifies the address for which routing information is displayed.
- **mask**—Specifies the network subnet mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 1–32)
- **longer-prefixes**—Specifies that the **address** and **mask** pair becomes a prefix and any routes that match that prefix are displayed.

Command Mode

EXEC mode

Example

The following example displays the current routing table state.

```
switchxxxxxx#  show ip route
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding:          enabled
Codes: C - connected, S - static, D - DHCP
S  0.0.0.0/0          [fe1/0/11] via  10.5.234.254  119:9:27   vlan 1
C  10.5.234.0/24      is directly connected               vlan 1
```

```
switchxxxxxx#  show ip route address 172.1.1.0 255.255.255.0
Codes: C - connected, S - static, E - OSPF external, * - candidate default
S 172.1.1.0/24 [fe1/0/13] via 10.0.2.1, 17:12:19, fe1/0/11
```

```
switchxxxxxx#  show ip route address 172.1.1.0 255.255.255.0
longer-prefixes
Codes: C - connected, S - static, E - OSPF external
S 172.1.1.0/24 [fe1/0/13] via 10.0.2.1, 17:12:19, fe1/0/11
S 172.1.1.1/32 [fe1/0/13] via 10.0.3.1, 19:51:18, fe1/0/11
```

The following table describes the significant fields shown in the display:

Field	Description
O	The protocol that derived the route.
10.8.1.0/24	The remote network address.
[30/2000]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.0.1.2	The address of the next router to the remote network.
00:39:08	The last time the route was updated in hours:minutes:seconds.
fe1/0/11	The interface through which the specified network can be reached.

43.9 show ip protocols

Use the **show ip protocols** EXEC mode command to display the parameters and current state of the active routing protocols.

Syntax

show ip protocols

Parameters

N/A

Default Usage

N/A

Command Mode

EXEC mode

Example

The following example displays the parameters and current state of the active routing protocols.

```
switchxxxxxx# show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds
Invalid after 180 seconds, hold down 120, flushed after 300
Redistributing: RIP, Static, OSPF
Default version control: send version 1, receive version 1
Interfaces:

Interface         Send              Receive      Key-chain
176.1.1.1         1                 1            flowers
176.2.1.1         passive           2

Routing Information Sources:
```

```
Gateway           Last Update
176.1.1.2         0:00:17
Preference: 60

Routing Protocol is "ospf"
Redistributing: OSPF, External direct, Static,
RIP
Interfaces:

Interface         Metric            Key-chain
176.1.1.1         10                flowers
176.2.1.1         1

Routing Information Sources:

Gateway           State
176.1.1.2         Full

External Preference: 60
Internal Preference: 20
```

43.10 show key-chains

Use the **show key chain** command in Privileged EXEC mode to display authentication key information,.

Syntax

show key chains [*name-of-chain*]

Parameters

name-of-chain—Name of the key chain to display, as named in the key chain command.

Default Configuration

Information about all key chains is displayed.

Command Mode

Privileged EXEC mode

Examples

Example 1 - The following is sample output from the show key chain command when the current time or date is defined:

```
Router# show key chain

Current Time of Date is Feb 8 2011

Key-chain trees:

  key 1 -- text "chestnut"

    accept lifetime (always valid) - (always valid) [valid now]

    send lifetime (always valid) - (always valid) [valid now]
```

key 2 -- text "birch"

accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)

send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)[valid now]

Example 2 - The following is sample output from the show key chain command when the current time or date is not defined:

Router# show key chain

Current Time of Date is not defined

Key-chain trees:

key 1 -- text "chestnut"

accept lifetime (always valid) - (always valid) [valid now]

send lifetime (always valid) - (always valid) [valid now]

key 2 -- text "birch"

accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)

send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)

43.11 show keys

Use the **show keys** Privileged EXEC mode command to display keys information.

Syntax

show keys [*key-id*]

Parameters

key-id—Specifies the identification number of an authentication key on a key chain. (Range: 1–255)

Default Usage

Display information for all keys.

Command Mode

Privileged EXEC mode

Example

The following example displays keys information.

```
switchxxxxxx# show keys

      key 1
                  accept:     13:30:00 Jan 25 2002 forever
                  send:       13:30:00 Jan 25 2002 forever
```

```
key 2
            accept:     13:30:00 Jan 25 2002 until 15:30:00
            send:       Jan 25 2002
                        14:00:00 Jan 25 2002 until 15:00:00
                        Jan 25 2002
key 3
            accept:     14:30:00 Jan 25 2002 until 16:30:00
            send:       Jan 25 2002
                        15:00:00 Jan 25 2002 until 16:00:00
                        Jan 25 2002
```

44 RIP Commands

44.1 router rip

The **router rip** Global Configuration mode command enables or disables RIP globally. The **no** format of the command disables RIP globally and removes its configuration.

Syntax

router rip

no router rip

Parameters

N/A

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

RIP supports the following global states:

- **disabled**
  RIP is not operational and cannot be configured. When this state is set, the RIP configuration is removed. This state can be set by the **no** router rip CLI command from any RIP global state.
- **enabled**
  RIP is operational, and can be configured. This state is set by the router rip CLI command from the **disabled** RIP global state and by the **no** shutdown CLI command from the **shutdown** RIP global state.
- **shutdown**
  RIP is not operational, but can be configured. When this state is set, the RIP configuration is not changed. This state can be set by the shutdown CLI command from the **enabled** RIP global state.

Example

The following example shows how to enable RIP globally:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)#
```

44.2 shutdown

The **shutdown** Router RIP configuration mode command sets the RIP global state to **shutdown**. The **no** format of the command sets the RIP global state to **enabled**.

Syntax
shutdown

no shutdown

Parameters
N/A

Default Configuration
Enabled

Command Mode
Router RIP configuration.

User Guidelines
Use the shutdown CLI command to disable RIP globally without removing its configuration.

Example
The following example shows how to disable RIP globally:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#shutdown
```

44.3 redistribute static
The **redistribute static** Router RIP configuration mode command enables RIP to advertise static routes. The **no** format of the command disables advertisement of static routes.

Syntax
redistribute static [**metric transparent**]

no redistribute static [**metric transparent**]

Parameters
metric transparent—Causes RIP to use the routing table metric for redistributing static routes as the RIP metric. If this parameter is omitted, the metric specified by the default-metric command is used.

Default Configuration
Static routes are not redistributed by RIP.

Command Mode
Router RIP configuration.

User Guidelines
If this command specifies the Metric Transparent mode, a static route is sent by RIP only if its metric is less than 16.

Use the **no redistribute static metric transparent** to change the metric of static redistributed routes to the default metric specified by the default-metric command.

Use the **no redistribute static** to disable distributing static routes by RIP.

Examples

Example 1.The following example enables redistribution of static routes by RIP with transparent metric:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#redistribute static metric transparent
exit
```

Example 2. The following example enables redistribution of static routes by RIP with transparent metric and then changes the metric to default:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#redistribute static metric transparent
switchxxxxxx(config-rip)#no redistribute static metric transparent
switchxxxxxx(config-rip)#exit
```

Example 3. The following example enables redistribution of static routes by RIP with the default metric and then changes the metric to transparent:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#redistribute static
switchxxxxxx(config-rip)#redistribute static metric transparent
switchxxxxxx(config-rip)#exit
```

Example 4. The following example enables redistribution of static routes by RIP with transparent metric. The second redistribute command has no effect.

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#redistribute static metric transparent
switchxxxxxx(config-rip)#redistribute static
switchxxxxxx(config-rip)#exit
```

Example 5. The following example disables redistribution of static routes by RIP:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#no redistribute static
switchxxxxxx(config-rip)#exit
```

44.4 default-metric

The **default-metric** Router RIP configuration mode command sets the default metric value when RIP advertises routes derived by other protocols or by static configuration. The **no** format of the command sets the default value.

Syntax
default-metric [*metric-value*]

no default-metric

Parameters
metric-value—Default metric value. Range 1-15.

Default Configuration
1.

Command Mode
Router RIP configuration.

Example
The following example shows how to set the default metric to 2:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#default-metric 2
```

44.5 network
The **network** Router RIP configuration mode command enables RIP on the given IP interfaces. The **no** format of the command disables RIP on the given IP interfaces and removes its interface configuration.

Syntax
network *ip-address*

no network *ip-address*

Parameters
ip-address—IP address of a switch's IP interface.

Default Configuration
N/A

Command Mode
Router RIP configuration.

User Guidelines
RIP can be defined only on manually-configured IP interfaces, meaning that RIP cannot be defined on an IP address defined by DHCP or on a default IP address.

Use the **no** network command to remove RIP on an IP interface and remove its interface configuration.

Example
The following example shows how to enable RIP on IP interface 1.1.1.1:

```
switchxxxxxx(config)#router rip
switchxxxxxx(config-rip)#network 1.1.1.1
```

44.6 clear statistics
The **clear statistics** Router RIP configuration mode command clears RIP statistics counters of all interfaces and all peers.

Syntax
clear statistics

Parameters
N/A

Default Configuration
N/A

Command Mode
Router RIP configuration mode

Example
The following example shows how to clear all counters:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-ip)# clear statistics
```

44.7 ip rip shutdown
The **ip rip shutdown** IP Interface configuration mode command changes the RIP state from **enabled** to **disabled** on an IP interface. The no format of the command returns the state to a value of **enabled**.

Syntax
ip rip shutdown

no ip rip shutdown

Parameters
N/A

Default Configuration
Enabled

Command Mode
IP Interface mode.

User Guidelines
Use the ip rip shutdown CLI command to disable RIP on an IP interface without removing its configuration.The **ip rip shutdown** command may be applied only to RIP interfaces created by the network command. The **ip rip shutdown** CLI command does not remove the RIP interface configuration.

Example
The following example shows how to disable RIP on the 1.1.1.1 IP interface:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)#ip rip shutdown
```

44.8 ip rip passive-interface
The **ip rip passive-interface** IP Interface Configuration mode command disables sending RIP packets on an IP interface. The **no** format of the command re-enables the sending of RIP packets.

Syntax
ip rip passive-interface

no ip rip passive-interface

Parameters
N/A.

Default Configuration
RIP messages are sent.

Command Mode
IP interface mode

Example
The following example shows how to stop transmitting RIP messages:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip passive-interface
```

44.9 ip rip default-information originate
The **ip rip default-information originate** IP Interface includes a default route in sent RIP messages. The **no** format of the command returns to default.

Syntax
ip rip default-information originate *metric*

no ip rip default-information originate

Parameters
metric—Default route metric value. Range 1-15.

Default Configuration
Default route is not generated by RIP.

Command Mode
IP Interface mode

Example
The following example shows how to enable sending of default route with metric 3:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip default-information originate 3
```

44.10 ip rip offset
The **ip rip offset** IP Configuration mode command defines a metric to add to incoming routes. The **no** format of the command returns to default.

Syntax
ip rip offset *offset*

no ip rip offset

Parameters
offset—Specifies the offset to be applied to received routes. Range: 1-15.

Default Configuration
1.

Command Mode
IP Interface mode

Example
The following example shows how to set offset to 2:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip offset 2
```

44.11 ip rip distribute-list in
The **ip rip distribute-list in** IP configuration mode command enables filtering of incoming routes. The **no** format of the command disables the filtering.

Syntax
ip rip distribute-list access *access-list-name* **in**

no ip rip distribute-list in

Parameters
access-list-name—Standard IP access list name, up to 32 characters. The list defines which networks are to be sent and which are to be suppressed.

Default Configuration
No filtering

Command Mode
IP interface mode

Example
The following example shows how to define input filtering using access list aaa:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip distribute-list aaa in
```

44.12 ip rip distribute-list out
The **ip rip distribute-list out** IP configuration mode command enables filtering of outgoing routes. The **no** format of the command disables the filtering.

Syntax
ip rip distribute-list access *access-list-name* **out**

no ip rip distribute-list out

Parameters
access-list-name—Standard IP access list name, up to 32 characters. The list defines which networks are to be sent and which are to be suppressed.

Default Configuration
No filtering

Command Mode
IP interface mode

Example
The following example shows how to define outgoing filtering using access list aaa:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip distribute-list aaa out
```

44.13 ip rip authentication mode

The **ip rip authentication mode** IP Interface Configuration mode command enables authentication. The **no** format of the command returns to default.

Syntax

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Parameters

- **text**—Specifies the clear text authentication.
- **md5**—Specifies the MD5 authentication.

Default Configuration

No authentication.

Command Mode

IP interface mode

User Guidelines

If you enable the MD5 authentication, you must configure a key chain name with the ip rip authentication key-chain Interface mode command. If a key chain is not defined for the IP interface or there is no valid key, RIP packets are not sent on the IP interface and received IP interface packets are dropped.

If you enable the clear text authentication, you must configure a password with the ip rip authentication-key Interface mode command. If a password is not defined for the IP interface then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

Example

The following example shows how to set the MD5 authentication mode:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
```

44.14 ip rip authentication key-chain

The **ip rip authentication key-chain** IP Interface Configuration mode command specifies the set of keys that can be used. The **no** format of the command returns to default.

Syntax

ip rip authentication key-chain *name-of-chain*

no ip rip authentication key-chain

Parameters

name-of-chain—Specifies the name of key set. The name-change parameter points to list of keys specified by the **key chain** command.

Default Configuration
No defined key chain.

Command Mode
IP Interface mode

User Guidelines
Only one key chain may be defined per IP interface. Each **ip rip authentication key-chain** command overrides the previous definition.

Example
The following example shows how to define a key chain name:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip authentication key-chain alpha
```

44.15 ip rip authentication-key
To assign a password to be used by neighboring routers that are using the RIP clear text authentication, use the **ip rip authentication-key** command in Interface Configuration mode. To remove a previously-assigned RIP password, use the **no** form of this command.

Syntax
ip rip authentication-key *password*

no ip rip authentication-key

Parameters
password—Any continuous string of characters that can be entered from the keyboard. Length: 1-8 characters.

Default Configuration
No password is specified.

Command Mode
IP Interface mode

User Guidelines
The password created by this command is used as a "key" that is inserted directly into the RIP header when the switch software builds routing protocol packets. A separate password can be assigned to each subnetwork. All neighboring routers on the same subnetwork must have the same password to be able to exchange RIP information.

Only one password may be defined per IP interface. Each **ip rip authentication-key** command overrides the previous definition.

Example
The following example shows how to define a password:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip rip authentication mode text
switchxxxxxx(config-ip)# ip rip authentication-key alph$$12
```

44.16 show ip rip database

The **show ip rip database** Privileged EXEC mode command displays information about the RIP database.

Syntax

show ip rip database [**all** | **brief** | *ip-address*]

Parameters

- **all**—Provides the full RIP database information about all RIP interfaces. The option is assumed if the parameter is omitted.
- **brief**—Provides a summary view of the RIP database information.
- **ip-address**—Provides the full RIP database information about the given IP Address.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

Example 1. The following example shows the full RIP database information about all RIP interfaces:

```
switchxxxxxx#show ip rip database
RIP is enabled
RIP Administrative state is UP
Redistributing is enabled from
  Static:
    Metric is transparent
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
IP Interface: 2.2.2.2
Administrative State is enabled
IP Interface Offset is 2
```

```
No Default Originate Metric
Authentication Type is MD5
Key Chain Name is chain1
No IN Filtering
Prefix List Name is PrefixList10
OUT Filtering Type is Access List
Access List Name is 12
IP Interface: 3.3.3.3
Administrative State is enabled
IP Interface Offset is 1
IP Interface is passive
No Default Originate Metric
No Authentication
No IN Filtering
No OUT Filtering
IP Interface: 4.4.4.4
Administrative State is shutdown
IP Interface Offset is 1
No Default Originate Metric
No Authentication
No IN Filtering
No OUT Filtering
```

Example 2. The following example shows the full RIP database information about a given IP address:

```
switchxxxxxx#show ip rip database 1.1.1.1
RIP is enabled
RIP Administrative state is UP
Redistributing is enabled from
  Static:
    Metric is transparent
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
```

Example 3. The following example shows the brief RIP database information about all RIP interfaces is displayed:

```
switchxxxxxx#show ip rip database brief
RIP is enabled
RIP Administrative state is UP
Redistributing is enabled from
  Static:
    Metric is transparent
IP Interface    Admin    Offset  Passive   Default Auth.  IN Filt. OUT Filt.
                State            Interface Origin. Type   Type     Type
                                           Metric
--------------- -------- ------- --------  ------- -----  -------  ---------
100.100.100.100 enabled    10      No          12   Text   Access   Access
2.2.2.2         enabled     2      No               MD5             Access
3.3.3.3         enabled     1      Yes
4.4.4.4         shutdown    1      No
```

Example 4. The following example shows the output when RIP is disabled:

```
switchxxxxxx#show ip rip database
RIP is disabled
```

44.17 show ip rip statistics

The **show ip rip statistics** Privileged EXEC mode command displays RIP Statistics.

Syntax

show ip rip statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#show ip rip statistics
RIP is enabled
Static redistributing is enabled with transparent metric
Default redistributing metric is 1
Interface     Received       Received           Sent
              Bad            Bad                Triggered
```

```
              Pakets          Routes              Packets
------------  -------------   -------------       -----------
1.1.1.1           -           1                   8
2.2.2.2           -           -                   7
```

44.18 show ip rip peers

The **show ip rip peers** Privileged EXEC mode command displays information about RIP peers.

Syntax

show ip rip peers

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx>show ip rip peers
RIP is enabled
Static redistributing is enabled with Default metric
Default redistributing metric is 1
Address       Last          Received       Received
              Update        Bad Packets    Bad Route
------------  ---------     ----------     ---------
1.1.12        00:10:17          -               1
2.2.2.3       00:10:01          -              -
```

45 ACL Commands

45.1 ip access-list

Use the **ip access-list extended** Global Configuration mode command to name an IPv4 access list (ACL) and to place the device in IPv4 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the permit (IP) and deny (IP) commands. The service-acl input command is used to attach this ACL to an interface.

Use the **no** form of this command to remove the access list.

Syntax

ip access-list extended *acl-name*

no ip access-list extended *acl-name*

Parameters

- **acl-name**—Name of the IPv4 access list. (Range 1-32 characters)

Default Configuration

No IPv4 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

An IPv4 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)#
```

45.2 permit (IP)

Use the **permit** IP Access-list Configuration mode command to set permit conditions for an IPv4 access list (ACL). Permit conditions are also known as access control entries (ACEs).

Syntax

permit *protocol {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**dscp** number | **precedence** number] [***time-range** time-range-name]*

permit *icmp {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**any** | icmp-type] [**any** | icmp-code]] [**dscp** number | **precedence** number] [**time-range** time-range-name]*

permit *igmp {**any** | source source-wildcard} {**any** | destination destination-wildcard}[igmp-type] [**dscp** number | **precedence** number]* **time-range** *time-range-name]*

permit tcp *{**any** | source source-wildcard} {**any**|source-port/port-range}{**any** | destination destination-wildcard} {**any**|destination-port/port-range} [**dscp** number | **precedence** number] [**match-all** list-of-flags] [**time-range** time-range-name]*

permit udp *{**any** | source source-wildcard} {**any**|source-port/port-range} {**any** | destination destination-wildcard} {**any**|destination-port/port-range} [**dscp** number | **precedence** number][**match-all** time-range-name] [**time-range** time-range-name]*

Parameters

- **permit** *protocol*—The name or the number of an IP protocol. Available protocol names are: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the **ip** keyword.(Range: 0–255)
- **source**—Source IP address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use ones in the bit position that you want to be ignored.
- **destination**—Destination IP address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use ones in the bit position that you want to be ignored.
- **dscp** *number*—Specifies the DSCP value.
- **precedence** *number*—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).(Range: 0–65535).
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all** *list-of-flags*—List of TCP flags that should occur. If a flag should be set, it is prefixed by “+”. If a flag should be unset, it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

After an ACE is added to an access control list, an implicit **deny any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in an ACE, it is not counted again, if it is also used for a source port in another ACE. If a range of ports is used for the destination port in an ACE, it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255
```

45.3 deny (IP)

Use the **deny** IP Access-list Configuration mode command to set deny conditions for IPv4 access list. Deny conditions are also known as access control entries (ACEs).

Syntax

deny *protocol {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**dscp** number | **precedence** number] [***time-range** time-range-name]*

deny *icmp {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**any** | icmp-type] [**any** | icmp-code]] [**dscp** number | **precedence** number] <all but Cisco> [**time-range** time-range-name]*

deny *igmp {**any** | source source-wildcard} {**any** | destination destination-wildcard}[igmp-type] [**dscp** number | **precedence** number] <all but Cisco>* **time-range** *time-range-name]*

deny tcp *{**any** | source source-wildcard} {**any**|source-port/port-range}{**any** | destination destination-wildcard} {**any**|destination-port/port-range} [**dscp** number | **precedence** number] [**match-all** list-of-flags] <all but Cisco> [**time-range** time-range-name]*

deny udp *{**any** | source source-wildcard} {**any**|source-port/port-range} {**any** | destination destination-wildcard} {**any**|destination-port/port-range} [**dscp** number | **precedence** number][**match-all** time-range-name] [**time-range** time-range-name]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. To match any protocol, use the Ip keyword. (Range: 0–255)
- **source**—Source IP address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source IP address. Use 1s in the bit position that you want to be ignored.
- **destination**—Destination IP address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination IP address. Use 1s in the bit position that you want to be ignored.
- **dscp** *number*—Specifies the DSCP value.
- **precedence** *number*—Specifies the IP precedence value.

- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **igmp-type**—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp 161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all** *list-of-flags*—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

After an ACE is added to an access control list, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for a source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port, it is counted again if it is also used for destination port.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255
```

45.4 ipv6 access-list (IPv6 extended)

Use the **ipv6 access-list** Global Configuration mode command to define an IPv6 access list (ACL) and to place the device in IPv6 Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are defined in the permit (IPv6) and deny (IPv6) commands. The service-acl input command is used to attach this ACL to an interface.

Use the **no** form of this command to remove the access list.

Syntax

ipv6 access-list [*acl-name]*

no ipv6 access-list *[acl-name]*

Parameters

- **acl-name**—Name of the IPv6 access list. Range 1-32 characters.

Default Configuration

No IPv6 access list is defined.

Command Mode

Global Configuration mode

User Guidelines

IPv6 ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Every IPv6 ACL has an implicit **permit icmp any any nd-ns any**, **permit icmp any any nd-na any**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.)

The IPv6 neighbor discovery process uses the IPv6 network layer service, therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, uses a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Example

```
Switch (config)# ipv6 access-list acl1
Switch(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

45.5 permit (IPv6)

Use the **permit** command in IPv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs.

Syntax

permit *protocol {**any** |{source-prefix/length}{**any** | destination- prefix/length} [**dscp** number | **precedence** number] [***time-range** time-range-name]*

permit icmp *{**any** | {source-prefix/length}{**any** | destination- prefix/length} {**any**|icmp-type} {**any**|icmp-code} [**dscp** number | **precedence** number] <all but Cisco> [**time-range** time-range-name]*

permit tcp *{**any** | {source-prefix/length} {**any** | source-port/port-range}}{**any** | destination-prefix/length} {**any**| destination-port/port-range} [**dscp** number | **precedence** number] [**match-all** list-of-flags] <all but Cisco> [**time-range** time-range-name]*

permit *udp {any | {source-prefix/length}} {any | source-port/port-range}}{any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number]<all but Cisco>[**time-range** time-range-name]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **dscp** *number*—Specifies the DSCP value. (Range: 0–63)
- **precedence** *number*—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)
- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all** *list-of-flag*—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default Configuration

No IPv6 access list is defined.

Command Mode

Ipv6 Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for a source port in ACE, it is not counted again if it is also used for a source port in another ACE. If a range of ports is used for destination port in ACE it is not counted again if it is also used for destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

Example

This example defines an ACL by the name of server and enters a rule (ACE) for tcp packets.

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit tcp 3001::2/64 any any 80
```

45.6 deny (IPv6)

Use the **deny** command in IPv6 Access List Configuration mode to set permit conditions (ACEs) for IPv6 ACLs.

Syntax

deny ***protocol*** *{**any** | {source-prefix/length}{**any** | destination- prefix/length} [**dscp** number | **precedence** number][**time-range** time-range-name] [**disable-port** | **log-input**]*

deny ***icmp*** *{**any** | {source-prefix/length}{any | destination- prefix/length} {**any**|icmp-type} {**any**|icmp-code} [**dscp** number | **precedence** number][**time-range** time-range-name] [**disable-port** | **log-input**]*

deny ***tcp*** *{**any** | {source-prefix/length} {**any** | source-port/port-range}}{**any** | destination-prefix/length} {**any**| destination-port/port-range} [**dscp** number | **precedence** number] [**match-all** list-of-flags][**time-range** time-range-name] [**disable-port** | **log-input**]*

deny ***udp*** *{**any** | {source-prefix/length}} {**any** | source-port/port-range}}{**any** | destination-prefix/length} {**any**| destination-port/port-range} [**dscp** number | **precedence** number]<[**time-range** time-range-name] [**disable-port** | **log-input**]*

Parameters

- **protocol**—The name or the number of an IP protocol. Available protocol names are: icmp (58), tcp (6) and udp (17). To match any protocol, use the ipv6 keyword. (Range: 0–255)
- **source-prefix/length**—The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **destination-prefix/length**—The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the format documented in RFC 3513 where the address is specified in hexadecimal using 16-bit values between colons.
- **dscp** *number*—Specifies the DSCP value. (Range: 0–63)
- **precedence** *number*—Specifies the IP precedence value.
- **icmp-type**—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report

(131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). (Range: 0–255)

- **icmp-code**—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- **destination-port**—Specifies the UDP/TCP destination port. You can enter a range of ports by using a hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data 20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- **source-port**—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all** *list-of-flags*—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Specifies to send an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No IPv6 access list is defined.

Command Mode

IPv6 Access-list Configuration mode

User Guidelines

The number of TCP/UDP ranges that can be defined in ACLs is limited. You can define up to #ASIC-specific ranges for TCP and up to #ASIC-specific ranges for UDP. If a range of ports is used for source port in ACE it is not counted again if it is also used for source port in another ACE. If a range of ports is used for a destination port in ACE it is not counted again if it is also used for a destination port in another ACE.

If a range of ports is used for source port it is counted again if it is also used for destination port.

Example

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

45.7 mac access-list

Use the **mac access-list** Global Configuration mode command to define a Layer 2 access list (ACL) based on source MAC address filtering and to place the device in MAC Access List Configuration mode. All commands after this command refer to this ACL. The rules (ACEs) for this ACL are

defined in the permit (MAC) and deny (MAC) commands. The service-acl input command is used to attach this ACL to an interface.

Use the **no** form of this command to remove the access list.

Syntax

mac access-list extended *acl-name*

no mac access-list extended *acl-name*

Parameters

acl-name—Specifies the name of the MAC ACL (Range: 1–32 characters).

Default Configuration

No MAC access list is defined.

Command Mode

Global Configuration mode

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

45.8 permit (MAC)

Use the **permit** command in MAC Access List Configuration mode to set permit conditions (ACEs) for a MAC ACL.

Syntax

permit *{**any** | source source-wildcard} {**any** | destination destination-wildcard} [eth-type 0 | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000**] [**vlan** vlan-id] [**cos** cos cos-wildcard] [**time-range** time-range-name]*

Parameters

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use 1s in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094)
- **cos**—The Class of Service of the packet. (Range: 0–7)
- **cos-wildcard**—Wildcard bits to be applied to the CoS.

- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

User Guidelines

After an access control entry (ACE) is added to an access control list, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
```

45.9 deny (MAC)

Use the **deny** command in MAC Access List Configuration mode to set deny conditions (ACEs) for a MAC ACL.

Syntax

deny *{**any** | source source-wildcard} {**any** | destination destination-wildcard} [{eth-type 0}| **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000**] [**vlan** vlan-id] [**cos** cos cos-wildcard]*[**time-range** *time-range-name] [**disable-port** | **log-input**]*

Parameters

- **source**—Source MAC address of the packet.
- **source-wildcard**—Wildcard bits to be applied to the source MAC address. Use ones in the bit position that you want to be ignored.
- **destination**—Destination MAC address of the packet.
- **destination-wildcard**—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- **eth-type**—The Ethernet type in hexadecimal format of the packet.
- **vlan-id**—The VLAN ID of the packet. (Range: 1–4094)
- **cos**—The Class of Service of the packet.(Range: 0–7)
- **cos-wildcard**—Wildcard bits to be applied to the CoS.
- **time-range-name**—Name of the time range that applies to this permit statement.(Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Sends an informational syslog message about the packet that matches the entry. Because forwarding is done in hardware and logging is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No MAC access list is defined.

Command Mode
MAC Access-list Configuration mode

User Guidelines
After an access control entry (ACE) is added to an access control list, an implicit **deny any any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

Example

```
switchxxxxxx(config)# mac access-list extended server1
switchxxxxxx(config-mac-al)# deny 00:00:00:00:00:01 00:00:00:00:00:ff any
```

45.10 service-acl input
Use the **service-acl input** command in interface Configuration mode to bind an access list(s) (ACL) to an interface.

Use the **no** form of this command to remove all ACLs from the interface.

Syntax
service-acl input *acl-name1 [acl-name2]*

no service-acl input

Parameters
acl-name—Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).

Default Configuration
No ACL is assigned.

Command Mode
Interface Configuration (Ethernet, Port-Channel) mode.

User Guidelines
The following rules govern when ACLs can be bound or unbound from an interface:

- IPv4 ACLs and IPv6 ACLs can be bound together to an interface.
- A MAC ACL cannot be bound on an interface which already has an IPv4 ACL or IPv6 ACL bound to it.
- Two ACLs of the same type cannot be bound to a port.
- An ACL cannot be bound to a port that is already bound to an ACL, without first removing the current ACL. Both ACLs must be mentioned at the same time in this command.

Example

```
switchxxxxxx(config)# mac access-list extended server-acl
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
```

```
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# service-acl input server-acl
```

45.11 service-acl output

Use the **service-acl output** command in Interface Configuration mode to control access to an interface on the Egress (transmit path). Use the **no** form of this command to remove the access control.

Syntax

service-acl output *acl-name1 [acl-name2]*
no service-acl *output*

Parameters

acl-name—Specifies an ACL to apply to the interface. See the usage guidelines. (Range: acl-name 0–32 characters. Use "" for empty string)

Default

No ACL is assigned.

Command Mode

Interface Configuration (Ethernet, Port-Channel) mode.

User Guidelines

The deny rule actions - **log-input** and **disable-port** are not supported. Trying to use these actions will result in an error.
IPv4 ACL and IPv6 ACL can be bound together on an interface.
A MAC ACL cannot be bound on an interface together with an IPv4 ACL or IPv6 ACL.
Two ACLs of the same type cannot be added to a port.
An ACL cannot be added to a port that is already bounded to an ACL, without first removing the current ACL and binding the two ACLs together.

Example

This example binds an Egress ACL to a port:

```
switchxxxxxx(config)# mac access-list extended server
switchxxxxxx(config-mac-al)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# interface fe1/0/11
switchxxxxxx(config-if)# service-acl output server
```

45.12 service-acl input block

Use the **service-acl input block** Interface Configuration mode commands to discard packets that are classified to specific protocols. Use the **no** form of those commands to disable discarding of the packets.

Syntax

service-acl input block *protocol1 [protocol2 … protocol6*]

no service-acl input

Parameters

protocol—Specifies a protocol to filter. Available values are: blockcdp, blockvtp, blockdtp, blockudld, blockpagp, blocksstp, and blockall.

Default Configuration

No protocol is defined.

Command Mode

Interface Configuration ((Ethernet, Port-Channel) mode

User Guidelines

If you want to define multiple protocols on the same interface, those protocols should be defined in the same command.

To change configuration of the protocol filtering for an interface, you should first remove the current assignment of protocol filtering assignment, and then assign the new configuration of the protocol filtering.

If Proprietary Protocol Filtering rules are assigned on an interface, the user is not able to assign ACL or Policy Map or Security suite rules to that interface and to enable 802.1X Dynamic Policy Assignment to that interface.

If ACL or Policy Map or Security suite rules are assigned to an interface or 802.1X Dynamic Policy Assignment is enabled for an interface, the user is not able to assign Proprietary Protocol Filtering rules to that interface.

The following table defines the DA and protocol types of the packets that are subject for discarding per each command:

Command	Destination Address	Protocol Type
blockcdp	0100.0ccc.cccc	0x2000
blockvtp	0100.0ccc.cccc	0x2003
blockdtp	0100.0ccc.cccc	0x2004
blockudld	0100.0ccc.cccc	0x0111
blockpagp	0100.0ccc.cccc	0x0104
blocksstp	0100.0ccc.cccd	-
blockall	0100.0ccc.ccc0 - 0100.0ccc.cccf	-

Example

```
switchxxxxxx(Config-if)# service-acl input blockcdp blockvtp
```

45.13 time-range

Use the **time-range** Global Configuration mode command to define time ranges for functionsor ACLs. In addition, this command enters the Time-range Configuration mode. All commands after this one refer to the time-range being defined.

This command sets a time-range name. Use the absolute and periodic commands to actually configure the time-range.

Use the **no** form of this command to remove the time range from the device.

Syntax

time-range *time-range-name*

no time-range *time-range-name*

Parameters

time-range-name—Specifies the name for the time range. (Range: 1–32 characters)

Default Configuration

No time range is defined

Command Mode

Global Configuration mode

User Guidelines

After the time-range command, use the absolute and periodic commands to actually configure the time-range. Multiple periodic commands are allowed in a time range. Only one absolute command is allowed.

If a time-range command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

All time specifications are interpreted as local time.

To ensure that the time range entries take effect at the desired times, the software clock should be set by the user or by SNTP. If the software clock is not set by the user or by SNTP, the time range ACEs are not activated.

The user cannot delete a time-range that is bound to any features, such as ACLs.

Example

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005 end 12:00 31 dec
2005 switchxxxxxx(config-time-range)# periodic monday 8:00 to friday 20:00
```

45.14 absolute

Use the **absolute** Time-range Configuration mode command to specify an absolute time when a time range is in effect. Use the **no** form of this command to remove the time limitation.

Syntax

absolute *start* *hh:mm day month year*

no absolute *start*

absolute *end* *hh:mm day month year*

no absolute *end*

Parameters

- **start**—Absolute time and date that the permit or deny statement of the associated function going into effect. If no start time and date are specified, the function is in effect immediately.
- **end**—Absolute time and date that the permit or deny statement of the associated function is no longer in effect. If no end time and date are specified, the function is in effect indefinitely.
- **hh:mm**—Time in hours (military format) and minutes (Range: 0–23, mm: 0–5)
- **day**—Day (by date) in the month. (Range: 1–31)
- **month**—Month (first three letters by name). (Range: Jan...Dec)
- **year**—Year (no abbreviation) (Range: 2000–2097)

Default Configuration

There is no absolute time when the time range is in effect.

Command Mode

Time-range Configuration mode

Example

```
switchxxxxxx(config)# time-range
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```

45.15 periodic

Use the **periodic** Time-range Configuration mode command to specify a recurring (weekly) time range for functions that support the time-range feature. Use the **no** form of this command to remove the time limitation.

Syntax

periodic *day-of-the-week hh:mm* ***to*** *day-of-the-week hh:mm*

no periodic *day-of-the-week hh:mm* ***to*** *day-of-the-week hh:mm*

periodic list *hh:mm* ***to*** *hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

no periodic list *hh:mm* ***to*** *hh:mm day-of-the-week1 [day-of-the-week2… day-of-the-week7]*

periodic list *hh:mm* ***to*** *hh:mm all*

no periodic list *all hh:mm* ***to*** *hh:mm all*

Parameters

- **day-of-the-week**—The starting day that the associated time range is in effect. The second occurrence is the ending day the associated statement is in effect. The second occurrence can

be the following week (see description in the User Guidelines). Possible values are: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.

- **hh:mm**—The first occurrence of this argument is the starting hours:minutes (military format) that the associated time range is in effect. The second occurrence is the ending hours:minutes (military format) the associated statement is in effect. The second occurrence can be at the following day (see description in the User Guidelines). (Range: 0–23, mm: 0–59)
- **list day-of-the-week1**—Specifies a list of days that the time range is in effect.

Default Configuration

There is no periodic time when the time range is in effect.

Command Mode

Time-range Configuration mode

User Guidelines

The second occurrence of the day can be at the following week, e.g. Thursday–Monday means that the time range is effective on Thursday, Friday, Saturday, Sunday, and Monday.

The second occurrence of the time can be on the following day, e.g. “22:00–2:00”.

Example

```
switchxxxxxx(config)# time-range
switchxxxxxx(config-time-range)# periodic Monday 12:00 to Wednesday 12:00
```

45.16 show time-range

Use the **show time-range** EXEC command to display the time range configuration.

Syntax

show time-range *time-range-name*

Parameters

time-range-name—Specifies the name of an existing time range.

Command Mode

EXEC mode

Example

```
switchxxxxxx# show time-range
http-allowed
--------------
absolute start 12:00 1 jan 2005
absolute end 12:00 31 dec 2005
periodic monday 8:00 to friday 20:00
```

45.17 show access-lists

Use the **show access-lists** Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

Syntax

show access-lists [*name*]

show access-lists ***time-range-active*** *[name]*

Parameters

- **name**—Specifies the name of the ACL.
- **time-range-active**—Shows only the Access Control Entries (ACEs) whose time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#show access-lists
Standard IP access list 1
deny   any any
Standard IP access list 2
deny   192.168.0.0/24
permit any any
Standard IP access list 3
deny   192.168.0.1 10.0.0.0/8
permit any any
Standard IP access list ACL1
permit 192.168.0.0/16 10.1.1.1
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any time-range weekdays
```

```
switchxxxxxx#show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8  0.0.0.0 any
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any time-range weekdays
```

```
switchxxxxxx#show access-lists ACL1
Standard IP access list ACL1
permit 0.0.0.0
```

```
permit 192.168.0.2, wildcard bits 0.0.0.255
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
permit 234 172.30.8.8  0.0.0.0 any
```

45.18 show interfaces access-lists

Use the **show interfaces access-lists** Privileged EXEC mode command to display access lists (ACLs) applied on interfaces.

Syntax

show interfaces access-lists *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, port-channel or VLAN.

Command Mode

Privileged EXEC mode

Example

```
Console# show interfaces access-lists
Interface Ingress ACL        Egress ACL
--------- -----------        ------------
fe1/0/11        ACL1               ACL2
fe1/0/12        ACL3
fe1/0/13        blockcdp, blockvtp
```

45.19 clear access-lists counters

Use the **clear access-lists counters** Privileged EXEC mode command to clear access-lists (ACLs) counters.

Syntax

clear access-lists counters *[interface-id]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear access-lists counters fe1/0/11
```

45.20 show interfaces access-lists counters

Use the **show interfaces access-lists counters** Privileged EXEC mode command to display Access List (ACLs) counters.

Syntax

show interfaces access-lists counters *[interface-id | port-channel-number]*

Parameters

interface-id—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

User Guidelines

The deny ACE hits count includes only ACEs with the log-input keyword.

Because forwarding is done in hardware and counting is done in software, if a large number of packets match a deny ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets are counted.

Example

```
switchxxxxxx# show interfaces access-lists counters
Interface             Deny ACE Hits
---------             -------------
fe1/0/11                   79
fe1/0/12                   9
fe1/0/13                   0
Number of hits that were counted in global counter (due to lack of resources) =19
```

46 Quality of Service (QoS) Commands

46.1 qos

Use the **qos** Global Configuration mode command to enable QoS on the device and set its mode. Use the **no** form of this command to disable QoS on the device.

Syntax

qos [***basic*** | ***advanced*** [***ports-not-trusted*** | ***ports-trusted***]]

no qos

Parameters

- **basic**—QoS basic mode. If no option is specified, the QoS mode defaults to the basic mode.
- **advanced**—Specifies the QoS advanced mode, which enables the full range of QoS configuration.
- **ports-not-trusted**—Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to egress queue 0. This is the default setting in advanced mode.
- **ports-trusted**—Relevant for advanced mode only. Indicates that packets, which are not classified by policy map rules to a QoS action, are mapped to an egress queue based on the packet's fields. Use the qos advanced-mode trust command to specify the trust mode.

Default Configuration

If **qos** is entered without any keywords, the QoS **basic** mode is **enabled**.

If **qos advanced** is entered without a keyword, the default is **ports-not-trusted**.

Command Mode

Global Configuration mode

Examples

Example 1- The following example enables QoS basic mode on the device.

```
switchxxxxxx(config)# qos
```

Example 2 - The following example enables QoS advanced mode on the device with the **ports-not-trusted** option.

```
switchxxxxxx(config)# qos advanced
```

46.2 qos advanced-mode trust

Use the **qos advanced-mode trust** Global Configuration command to configure the trust mode in advanced mode. Use the **no** form of this command to return to default.

Syntax

qos advanced-mode trust {*cos* | *dscp* | *cos-dscp*}

no qos advanced-mode trust

Parameters

- **cos**—Classifies ingress packets with the packet CoS values. For untagged packets, the port default CoS is used.
- **dscp**—Classifies ingress packets with the packet DSCP values.
- **cos-dscp**—Classifies ingress packets with the packet DSCP values for IP packets. For other packet types, use the packet CoS values.

Default Configuration

cos-dscp

Command Mode

Global Configuration

User Guidelines

The configuration is relevant for advanced mode in the following cases:

- **ports-not-trusted mode:** For packets that are classified to the QoS action trust.
- **ports-trusted mode:** For packets that are not classified by to any QoS action or classified to the QoS action trust.

Example

The following example sets **cos** as the trust mode for QoS on the device.

```
switchxxxxxx(config)# qos advanced-mode trust cos
```

46.3 show qos

Use the **show qos** EXEC mode command to display the QoS information for the device. The trust mode is displayed for the QoS basic mode.

Syntax

show qos

Parameters

N/A

Default Configuration

Disabled Command Mode

Command Mode

EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode.

Examples

Example 1 - The following example displays QoS attributes when QoS is enabled in basic mode and the advanced mode is supported.

```
switchxxxxxx#  show qos
Qos: basic
Basic trust: dscp
```

Example 2 - The following example displays QoS attributes when QoS is enabled in basic mode on the device and the advanced mode is not supported.

```
switchxxxxxx#  show qos
Qos: disable
Trust: dscp
```

46.4 class-map

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally-named service policy applied on a per-interface basis.

A class map consists of one or more ACLs (see ACL Commands). It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

Use the **class-map** Global Configuration mode command to create or modify a class map and enter the Class-map Configuration mode (only possible when QoS is in the advanced mode).

Use the **no** form of this command to delete a class map.

All class map commands are only available when QoS is in advanced mode.

Syntax

class-map *class-map-name* ***[match-all | match-any]***

no class-map *class-map-name*

Parameters

- **class-map-name**—Specifies the class map name.
- **match-all**—Performs a logical AND of all the criteria of the ACLs belonging to this class map. All match criteria in this class map must be matched.
- **match-any**—Performs a logical OR of the criteria of the ACLs belonging to this class map. Only a single match criteria in this class map must be matched.

Default Configuration

If neither **match-all** nor **match-any** is specified, the **match-all** parameter is selected by default.

Command Mode

Global Configuration mode

User Guidelines

The **class-map** enters Class-map Configuration mode. In this mode, up to two **match** commands can be entered to configure the criteria for this class. Each **match** specifies an ACL.

When using two **match** commands, each must point to a different type of ACL, such as: one IP ACL and one MAC ACL. The classification is by first match, therefore, the order of the ACLs is important.

Error messages are generated in the following cases:

- There is more than one **match** command in a **match-all** class map
- There is a repetitive classification field in the participating ACLs.

After entering the Class-map Configuration mode, the following configuration commands are available:

- **exit**: Exits the Class-map Configuration mode.
- **match**: Configures classification criteria.
- **no**: Removes a match statement from a class map.

Example

The following example creates a class map called Class1 and configures it to check that packets match all classification criteria in the ACL specified.

```
switchxxxxxx(config)# class-map class1 match-all
switchxxxxxx(config-cmap)#match access-group acl-name
```

46.5 show class-map

The **show class-map** EXEC mode command displays all class maps when QoS is in advanced mode.

Syntax

show class-map [*class-map-name*]

Parameters

class-map-name—Specifies the name of the class map to be displayed.

Command Mode

EXEC mode

Example

The following example displays the class map for Class1.

```
switchxxxxxx#  show class-map class1
Class Map match-any class1 (id4)
Match IP dscp 11 21
```

46.6 match

Use the **match** Class-map Configuration mode command to bind the ACLs that belong to the class-map being configured. Use the **no** form of this command to delete the ACLs.

This command is available only when the device is in QoS advanced mode.

Syntax
match access-group *acl-name*

no match access-group *acl-name*

Parameters
acl-name—Specifies the MAC or IP ACL name.

Default Configuration
No match criterion is supported.

Command Mode
Class-map Configuration mode.

Example
The following example defines a class map called Class1. Class1 contains an ACL called **enterprise**. Only traffic matching all criteria in **enterprise** belong to the class map.

```
switchxxxxxx(config)# class-map class1
switchxxxxxx(config-cmap)# match access-group enterprise
```

46.7 policy-map
A policy map contains one or more class maps and an action that is taken if the packet matches the class map. Policy maps may be bound to ports/port-channels.

Use the **policy-map** Global Configuration mode command to creates a policy map and enter the Policy-map Configuration mode. Use the **no** form of this command to delete a policy map.

This command is only available when QoS is in advanced mode.

Syntax
policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters
policy-map-name—Specifies the policy map name.

Default Configuration
N/A

Command Mode
Global Configuration mode

User Guidelines
Use the **policy-map** Global Configuration mode command to specify the name of the policy map to be created, added to, or modified before configuring policies for classes whose match criteria are defined in a class map.

Entering the policy-map Global Configuration mode command also enables configuring or modifying the class policies for that policy map. Class policies in a policy map can be configured only if the classes have match criteria defined for them.

Policy map is applied on the ingress path.

The match criteria is for a class map. Only one policy map per interface is supported. The same policy map can be applied to multiple interfaces and directions.

The service-policy command binds a policy map to a port/port-channel.

Example

The following example creates a policy map called Policy1 and enters the Policy-map Configuration mode.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)#
```

46.8 class

Use the **class** Policy-map Configuration mode command after the policy-map command to attach ACLs to a policy-map.

Use the **no** form of this command to detach a class map from a policy map.

This command is only available when QoS is in advanced mode.

Syntax

class *class-map-name [***access-group** *acl-name*]

no class *class-map-name*

Parameters

- **class-map-name**—Specifies the name of an existing class map. If the class map does not exist, a new class map is created under the specified name.
- **access-group** *acl-name*—Specifies the name of an IP or MAC Access Control List (ACL).

Default Configuration

No class map is defined for the policy map.

Command Mode

Policy-map Configuration mode

User Guidelines

This is the same as creating a class map and then binding it to the policy map.

You can specify an existing class map in this command, or you can use the **access-group** parameter to create a new class map.

After the policy-map is defined, use the service-policy command to attach it to a port/port-channel.

Example
The following example defines a traffic classification (class map) called **class1** containing an ACL called **enterprise**. The class is in a policy map called **policy1**. The policy-map **policy1** now contains the ACL **enterprise**.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1 access-group enterprise
```

46.9 show policy-map
Use the **show policy-map** EXEC mode command to display all policy maps or a specific policy map.

This command is only available when QoS is in advanced mode.

Syntax
show policy-map [*policy-map-name*]

Parameters
policy-map-name—Specifies the policy map name.

Default Configuration
All policy-maps are displayed.

Command Mode
EXEC mode

Example
The following example displays all policy maps.

```
switchxxxxxx#  show policy-map
Policy Map policy1
class class1
set IP dscp 7
Policy Map policy2
class class 2
police 96000 4800 exceed-action drop
class class3
police 124000 96000 exceed-action policed-dscp-transmit
```

46.10 trust
Use the **trust** Policy-map Class Configuration mode command to configure the trust state. This command is relevant only when QoS is in advanced, ports-not-trusted mode. Trust indicates that traffic is sent to the queue according to the packet's QoS parameters (UP or DSCP).

Use the **no** form of this command to return to the default trust state.

This command is only available when QoS is in advanced mode.

Syntax

trust

no trust

Parameters

N/A

Default Configuration

The default state is according to the mode selected in the qos command (advanced mode). The type of trust is determined in qos advanced-mode trust.

Command Mode

Policy-map Class Configuration mode

User Guidelines

Use this command to distinguish the QoS trust behavior for certain traffic from others. For example, incoming traffic with certain DSCP values can be trusted. A class map can be configured to match and trust the DSCP values in the incoming traffic.

The type of trust is determined in qos advanced-mode trust.

Trust values set with this command supersede trust values set on specific interfaces with the qos trust (Interface) Interface Configuration mode command.

The trust and set commands are mutually exclusive within the same policy map.

Policy maps, which contain **set** or **trust** commands or that have ACL classification to an egress interface, cannot be attached by using the service-policy Interface Configuration mode command.

If specifying **trust cos**, QoS maps a packet to a queue, the received or default port CoS value, and the CoS-to-queue map.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and configures the trust state using the DSCP value in the ingress packet.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-mac-al)# permit ip any any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# trust
```

46.11 set

Use the **set** Policy-map Class Configuration mode command to select the value that QoS uses as the DSCP value, the egress queue or to set user priority values.

This command is only available when QoS is in advanced mode.

Syntax

set *{**dscp** new-dscp* | ***queue** queue-id* | ***cos** new-cos}*

no set

Parameters

- **dscp** *new-dscp*—Specifies the new DSCP value for the classified traffic. (Range: 0–63)
- **queue** *queue-id*—Specifies the egress queue. (Range: 1-8)
- **cos** *new-cos*—Specifies the new user priority to be marked in the packet. (Range: 0–15)

Command Mode

Policy-map Class Configuration mode

User Guidelines

The set and trust commands are mutually exclusive within the same policy map.

To return to the Configuration mode, use the **exit** command. To return to the Privileged EXEC mode, use the **end** command.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the DSCP value in the packet to 56 for classes in the policy map called p1.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-mac-al)# permit ip any any
switchxxxxxx(config-mac-al)# exit
switchxxxxxx(config)# class-map c1
switchxxxxxx(config-cmap)# match access-group ip1
switchxxxxxx(config-cmap)# exit
switchxxxxxx(config)# policy-map p1
switchxxxxxx(config-pmap)# class c1
switchxxxxxx(config-pmap-c)# set dscp 56
```

46.12 police

Use the **police** Policy-map Class Configuration mode command to define the policer for classified traffic. This defines another group of actions for the policy map (per class map).

This command is used after the policy-map and class commands.

Use the **no** form of this command to remove a policer.

This command is only available when QoS is in advanced mode.

Syntax

police *committed-rate-kbps committed-burst-byte **[exceed-action** {**drop** | **policed-dscp-transmit**}]*

no police

Parameters

- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (bps).(Range: 3–10000000)
- **committed-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action** {**drop** | **policed-dscp-transmit**}—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP, according to the policed-DSCP map as configured by the **qos map policed-dscp** Global Configuration mode command.

Default Usage

N/A

Command Mode

Policy-map Class Configuration mode

User Guidelines

This command only exists in when the device is in Layer 2 mode.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

Example

The following example defines a policer for classified traffic. When the traffic rate exceeds 124,000 kbps and the normal burst size exceeds 9600 bytes, the packet is dropped. The class is called class1 and is in a policy map called policy1.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action drop
```

46.13 service-policy

Use the **service-policy** Interface Configuration (Ethernet, Port-channel) mode command to bind a policy map to a port/port-channel. Use the **no** form of this command to detach a policy map from an interface.

This command is only available in QoS advanced mode.

Syntax

service-policy input *policy-map-name*

no service-policy input

Parameters

policy-map-name—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

User Guidelines
Only one policy map per interface per direction is supported.

Example
The following example attaches a policy map called Policy1 to the input interface.

```
switchxxxxxx(config-if)# service-policy input policy1
```

46.14 qos aggregate-policer
Use the **qos aggregate-policer** Global Configuration mode command to define the policer parameters that can be applied to multiple traffic classes. Use the **no** form of this command to remove an existing aggregate policer.

This command is only available when QoS is in advanced mode.

Syntax
qos aggregate-policer *aggregate-policer-name committed-rate-kbps excess-burst-byte* [***exceed-action*** *{**drop** | **policed-dscp-transmit**}]*

no qos aggregate-policer *aggregate-policer-name*

Parameters
- **aggregate-policer-name**—Specifies the aggregate policer name.
- **committed-rate-kbps**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3–57982058)
- **excess-burst-byte**—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action** {***drop*** | ***policed-dscp-transmit***}—Specifies the action taken when the rate is exceeded. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP.

Default Configuration
No aggregate policer is defined.

Command Mode
Global Configuration mode

User Guidelines
This command only exists when the device is in Layer 2.

Define an aggregate policer if the policer aggregates traffic from multiple class maps.

Aggregate policers cannot aggregate traffic from multiple devices. If the aggregate policer is applied to more than one device, the traffic on each device is counted separately and is limited per device.

Traffic from two different ports on the same device can be aggregated for policing purposes.

An aggregate policer can be applied to multiple classes in the same policy map.

An aggregate policer cannot be deleted if it is being used in a policy map. The **no police aggregate** Policy-map Class Configuration mode command must first be used to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** command.

Policing uses a token bucket algorithm. CIR represents the speed with which the token is added to the bucket. CBS represents the depth of the bucket.

Example

The following example defines the parameters of a policer called Policer1 that can be applied to multiple classes in the same policy map. When the average traffic rate exceeds 124,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600
exceed-action drop
```

46.15 show qos aggregate-policer

Use the **show qos aggregate-policer** EXEC mode command to display aggregate policers

This command is only available in QoS advanced mode.

Syntax

show qos aggregate-policer [*aggregate-policer-name*]

Parameters

aggregate-policer-name—Specifies the aggregate policer name.

Default Configuration

All policers are displayed.

Command Mode

EXEC mode

Example

The following example displays the parameters of the aggregate policer called Policer1.

```
switchxxxxxx#  show qos aggregate-policer policer1
aggregate-policer policer1 96000 4800 exceed-action drop
not used by any policy map
```

46.16 police aggregate

Use the **police aggregate** Policy-map Class Configuration mode command to apply an aggregate policer to multiple class maps within the same policy map. Use the **no** form of this command to remove an existing aggregate policer from a policy map.

This command is only available in QoS advanced mode.

Syntax

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Parameters

aggregate-policer-name—Specifies the aggregate policer name.

Command Mode

Policy-map Class Configuration mode

User Guidelines

An aggregate policer can be applied to multiple classes in the same policy map. An aggregate policer cannot be applied across multiple policy maps or interfaces.

Use the **exit** command to return to the Configuration mode. Use the **end** command to return to the Privileged EXEC mode.

Example

The following example applies the aggregate policer called Policer1 to a class called class1 in a policy map called policy1 and class2 in policy map policy2.

```
switchxxxxxx(config)# qos aggregate-policer policer1 124000 9600
exceed-action drop
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class class1
switchxxxxxx(config-pmap-c)# police aggregate policer1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)# policy-map policy2
switchxxxxxx(config-pmap)# class class2
switchxxxxxx(config-pmap-c)# police aggregate policer1
```

46.17 wrr-queue cos-map

Use the **wrr-queue cos-map** Global Configuration mode command to map Class of Service (CoS) values to a specific egress queue. Use the **no** form of this command to restore the default configuration.

Syntax

wrr-queue cos-map *queue-id cos0... cos7*

no wrr-queue cos-map [*queue-id*]

Parameters

- **queue-id**—Specifies the queue number to which the CoS values are mapped.
- **cos0... cos**7—Specifies up to 8 CoS values to map to the specified queue number. (Range: 0–7)

Default Configuration
[8 queues]The default CoS value mapping to 8 queues is as follows:

CoS value 0 is mapped to queue 3.

CoS value 1 is mapped to queue 1.

CoS value 2 is mapped to queue 2.

CoS value 3 is mapped to queue 4.

CoS value 4 is mapped to queue 5.

CoS value 5 is mapped to queue 6.

CoS value 6 is mapped to queue 7.

CoS value 7 is mapped to queue 8.

Command Mode
Global Configuration mode

User Guidelines
Use this command to distribute traffic to different queues.

Example
The following example maps CoS value 4 and 6 to queue 2.

```
switchxxxxxx(config)# wrr-queue cos-map 2 4 6
```

46.18 wrr-queue bandwidth
Use the **wrr-queue bandwidth** global Configuration command to assign Weighted Round Robin (WRR) weights to egress queues. The weight ratio determines the frequency at which the packet scheduler removes packets from each queue. Use the **no** form of this command to restore the default configuration.

Syntax
wrr-queue bandwidth *weight1 weight2... weighting*

no wrr-queue bandwidth

Parameters
weight1 weight1... weighting the ratio of bandwidth assigned by the WRR packet scheduler to the packet queues. See explanation in the User Guidelines. Separate each value by a space. (Range for each weight: 0–255)

Default Configuration
wrr is disabled by default. The default wrr weight is '1' for all queues.

Command Mode
Global Configuration mode

User Guidelines

The ratio for each queue is defined as the queue weight divided by the sum of all queue weights (the normalized weight). This sets the bandwidth allocation of each queue.

A weight of 0 indicates that no bandwidth is allocated for the same queue, and the shared bandwidth is divided among the remaining queues. It is not recommended to set the weight of a queue to a 0 as it might stop transmission of control-protocols packets generated by the device.

All 7 queues participate in the WRR, excluding the expedite queues, whose corresponding weight is not used in the ratio calculation.

An expedite queue is a priority queue, which is serviced until empty before the other queues are serviced. The expedite queues are designated by the priority-queue out num-of-queues command.

Example

The following assigns WRR values to the queues.

```
switchxxxxxx(config)# wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

46.19 priority-queue out num-of-queues

An expedite queue is a strict priority queue, which is serviced until empty before the other lower priority queues are serviced.

Use the **priority-queue out num-of-queues** Global Configuration mode command to configure the number of expedite queues. Use the **no** form of this command to restore the default configuration.

Syntax

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

Parameters

- **number-of-queues**—Specifies the number of expedite (strict priority) queues. Expedite queues are assigned to the queues with the higher indexes. (Range: 0–8).

  There must be either 0 wrr queues or more than one.
- If **number-of-queues** = 0, all queues are assured forwarding (according to wrr weights) If the **number-of-queues** = 8, all queues are expedited (strict priority queues).

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

the weighted round robin (WRR) weight ratios are affected by the number of expedited queues, because there are fewer queues participating in WRR. This indicates that the corresponding weight in the **wrr-queue bandwidth** Interface Configuration mode command is ignored (not used in the ratio calculation).

Example
The following example configures the number of expedite queues as 2.

```
switchxxxxxx(config)# priority-queue out num-of-queues 2
```

46.20 traffic-shape
The egress port shaper controls the traffic transmit rate (Tx rate) on a port.

Use the **traffic-shape** Interface Configuration mode command to configure the egress port shaper. Use the **no** form of this command to disable the shaper.

Syntax
traffic-shape *committed-rate* [*committed-burst*]

no traffic-shape

Parameters
- **committed-rate**—Specifies the maximum average traffic rate (CIR) in kbits per second (kbps). (Range: FE, GE: 64kbps–maximum port speed; 10GE: 64Kbps–maximum port speed)
- **committed-burst**—Specifies the maximum permitted excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration
The shaper is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example sets a traffic shaper on `fe1/0/15` on queue 1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# traffic-shape 1 124000 9600
```

46.21 traffic-shape queue
The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on a port.

Use the **traffic-shape queue** Interface Configuration mode command to configure the egress queue shaper. Use the **no** form of this command to disable the shaper.

Syntax
traffic-shape queue *queue-id committed-rate* [*committed-burst*]

no traffic-shape queue *queue-id*

Parameters
- **queue-id**—Specifies the queue number to which the shaper is assigned. (Range: 1-4)

- **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 64 kbps–maximum port speed)
- **committed-burst**—Specifies the excess burst size (CBS) in bytes. (Range: 4096 - 16762902 bytes)

Default Configuration
The shaper is disabled.

Command Mode
Interface Configuration (Ethernet, Port-channel) mode

Example
The following example sets a shaper on queue 1 on `fe1/0/15` when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# traffic-shape 1 124000 9600
```

46.22 rate-limit (Ethernet)
Use the **rate-limit** Interface Configuration mode command to limit the incoming traffic rate on a port. Use the **no** form of this command to disable the rate limit.

Syntax
rate-limit *committed-rate-kbps [**burst** committed-burst-bytes]*

no rate-limit

Parameters
- **committed-rate-kbps**—Specifies the maximum number of kilobits per second of ingress traffic on a port. The range is 3– max port speed.
- ***burst committed-burst-bytes***—The burst size in bytes (3000–19173960). If unspecified, defaults to 128K.

Default Configuration
Rate limiting is disabled.

Committed-burst-bytes is 128K.

Command Mode
Interface Configuration (Ethernet) mode

User Guidelines
Storm control and rate-limit (of Unicast packets) cannot be enabled simultaneously on the same port.

Example
The following example limits the incoming traffic rate on `fe1/0/1`5 to 150,000 kbps.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# rate-limit 150000
```

46.23 rate-limit (VLAN)

Use the Layer 2 **rate-limit** (VLAN) Global Configuration mode command to limit the incoming traffic rate for a VLAN. Use the **no** form of this command to disable the rate limit.

Syntax

rate-limit *vlan-id committed-rate committed-burst*

no rate-limit vlan

Parameters

- **vlan-id**—Specifies the VLAN ID.
- **committed-rate**—Specifies the average traffic rate (CIR) in kbits per second (kbps). (Range: 3-57982058)
- **committed-burst**—Specifies the maximum burst size (CBS) in bytes. (Range: 3000-19173960)

Default Configuration

Rate limiting is disabled.

Committed-burst-bytes is 128K.

Command Mode

Global Configuration mode

User Guidelines

The rate limit is calculated separately for each unit in a stack, and for each packet processor in a unit.

Traffic policing in a policy map takes precedence over VLAN rate limiting. If a packet is subject to traffic policing in a policy map and is associated with a VLAN that is rate limited, the packet is counted only in the traffic policing of the policy map.

This command does not work in Layer 3 mode.

Example

The following example limits the rate on VLAN 11 to 150000 kbps or the normal burst size to 9600 bytes.

```
switchxxxxxx(config)# rate-limit 11 150000 9600
```

46.24 qos wrr-queue wrtd

Use the **qos wrr-queue wrtd** Global Configuration mode command to enable Weighted Random Tail Drop (WRTD). Use the **no** form of this command to disable WRTD.

Syntax

qos wrr-queue wrtd

no qos wrr-queue wrtd

Parameters
N/A

Default
Disabled

Command Mode
Global Configuration mode

User Guidelines
The command is effective after reset.

Example

```
switchxxxxxx(conf)#>qos wrr-queue wrtd
This setting will take effect only after copying running configuration to startu
p configuration and resetting the device
switchxxxxxx(config)#
```

46.25 show qos wrr-queue wrtd

Use the **show qos wrr-queue wrtd** Exec mode command to display the Weighted Random Tail Drop (WRTD) configuration.

Syntax
show qos wrr-queue wrtd

Parameters
N/A

Default Configuration
N/A

Command Mode
Exec mode

Example

```
switchxxxxxx#  show qos wrr-queue wrtd
 Weighted Random Tail Drop is disabled
 Weighted Random Tail Drop will be enabled after reset
```

46.26 show qos interface

Use the **show qos interface** EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

show qos interface [***buffers*** | ***queueing*** | ***policers*** | ***shapers*** | ***rate-limit]*** *[interface-id]*

Parameters

- **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the 8 queues. For FE ports, displays the minimum reserved setting.
- **queueing**—Displays the queue's strategy (WRR or EF), the weight for WRR queues, the CoS to queue map and the EF priority.
- **policers**—Displays all the policers configured for this interface, their settings, and the number of policers currently unused (on a VLAN).
- **shapers**—Displays the shaper of the specified interface and the shaper for the queue on the specified interface.
- **rate-limit**—Displays the rate-limit configuration.
- **interface-id**—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, or Port-channel.

Default Configuration

N/A

Command Mode

EXEC mode

User Guidelines

If no parameter is specified with the **show qos interface** command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so on), default CoS value, DSCP-to-DSCP- map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Examples

Example 1 - This is an example of the output from the **show qos interface buffers** command for 8 queues.

```
switchxxxxxx#show qos interface buffers fe1/0/11
fe1/0/11
Notify Q depth:
buffers fe1/0/11
Ethernet fe1/0/11
qid  thresh0  thresh1  thresh2
1    100      100      80
2    100      100      80
3    100      100      80
4    100      100      80
5    100      100      80
6    100      100      80
7    100      100      80
8    100      100      80
```

Example 2 - This is an example of the output from the **show qos interface shapers** command.

```
switchxxxxxx#show qos interface shapers fe1/0/11
fe1/0/11
Port shaper: enable
Committed rate: 192000 bps
Committed burst: 9600 bytes

                Target                  Target
QID   Status    Committed               Committed
                Rate [bps]              Burst [bytes]
1     Enable    100000                  17000
2     Disable   N/A                     N/A
3     Enable    200000                  19000
4     Disable   N/A                     N/A
5     Disable   N/A                     N/A
6     Disable   N/A                     N/A
7     Enable    178000                  8000
8     Enable    23000                   1000
```

Example - 3 This is an example of the output from the **show qos interface policer** command.

```
switchxxxxxx#  show qos interface policer fe1/0/11
Ethernet fe1/0/11
Class map: A
Policer type: aggregate
Commited rate: 192000 bps
Commited burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Commited rate: 192000 bps
Commited burst: 9600 bytes
Exceed-action: drop
Class map: C
Policer type: none
Commited rate: N/A
Commited burst: N/A
Exceed-action: N/A
```

Example 4 - This is an example of the output from the **show qos interface rate-limit** command.

```
switchxxxxxx#  show qos interface rate-limit fe1/0/11

Port          rate-limit [kbps]         Burst [KBytes]
-----         -----------------         --------------
fe1/0/11      1000                      512K
```

46.27 wrr-queue

Use the **wrr-queue** Global Configuration mode command to enable the tail-drop mechanism on an egress queue. Use the **no** form of this command to disable the tail-drop mechanism on an egress queue.

Syntax

wrr-queue ***tail-drop***

no wrr-queue

Parameters

tail-drop— Specifies the tail-drop mechanism.

Default Configuration

The tail-drop mechanism on an egress queue i

s disabled.

Command Mode

Global Configuration mode

User Guidelines

This command can only be used if Advanced mode is enabled.

Example

The following example enables the tail-drop mechanism on an egress queue.

```
switchxxxxxx(config)# wrr-queue tail-drop
```

46.28 qos wrr-queue threshold

Use the **qos wrr-queue threshold** Global Configuration mode command to assign queue thresholds globally. Use the **no** form of this command to restore the default configuration.

This command is only available in QoS advanced mode.

Syntax

qos wrr-queue threshold gigabitethernet tengigabitethernet *queue-id threshold-percentage*

no qos wrr-queue threshold gigabitethernet *queue-id*

Parameters

- **gigabitethernet**—Specifies that the thresholds are to be applied to Gigabit Ethernet ports.
- **tengigabitethernet**—Specifies that the thresholds are to be applied to 10 Gigabit Ethernet ports.
- **queue-id**—Specifies the queue number to which the tail-drop threshold is assigned.
- **threshold-percentage**—Specifies the queue threshold percentage value.

Default Configuration
The default threshold is 80 percent.

Command Mode
Global Configuration mode

User Guidelines
If the threshold is exceeded, packets with the corresponding Drop Precedence (DP) are dropped until the threshold is no longer exceeded.

Example
The following example assigns a threshold of 80 percent to WRR queue 1.

```
switchxxxxxx(config)# qos wrr-queue threshold gigabitethernet 1 80
```

46.29 qos map policed-dscp
Use the **qos map policed-dscp** Global Configuration mode command to configure the policed-DSCP map for remarking purposes. Use the **no** form of this command to restore the default configuration.

This command is only available in QoS advanced mode.

Syntax
qos map policed-dscp *dscp-list* ***to*** *dscp-mark-down*

no qos map policed-dscp [*dscp-list*]

Parameters
- **dscp- list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0–63)
- **dscp-mark-down**—Specifies the DSCP value to mark down. (Range: 0–63)

Default Configuration
The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode
Global Configuration mode.

User Guidelines
The original DSCP value and policed-DSCP value must be mapped to the same queue in order to prevent reordering.

Example
The following example marks incoming DSCP value 3 as DSCP value 5 on the policed-DSCP map.

```
switchxxxxxx(config)# qos map policed-dscp 3 to 5
```

46.30 qos map dscp-queue

Use the **qos map dscp-queue** Global Configuration mode command to configure the DSCP to CoS map. Use the **no** form of this command to restore the default configuration.

Syntax

qos map dscp-queue *dscp-list* to *queue-id*

no qos map dscp-queue [*dscp-list*]

Parameters

- **dscp-list**—Specifies up to 8 DSCP values, separated by spaces. (Range: 0– 63)
- **queue-id**—Specifies the queue number to which the DSCP values are mapped.

.Default Configuration

The default map for 8 queues is as follows.

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-56	57-63
Queue-ID	1	2	3	4	5	6	7	8

Command Mode

Global Configuration mode

Example

The following example maps DSCP values 33, 40 and 41 to queue 1.

```
switchxxxxxx(config)# qos map dscp-queue 33 40 41 to 1
```

46.31 qos map dscp-dp

Use the **qos map dscp-dp** Global Configuration mode command to map the DSCP values to Drop Precedence. Use the **no** form of this command to restore the default configuration.

This command is only available in QoS advanced mode.

Syntax

qos map dscp-dp *dscp-list* to *dp*

no qos map dscp-dp [*dscp-list*]

Parameters

- **dscp-list**—Specifies up to 8 DSCP values, with values separated by a space. (Range: 0–63)
- **dp**—Specifies the Drop Precedence value to which the DSCP values are mapped. (values: 0,2) where 2 is the highest Drop Precedence).

Default Configuration

All the DSCPs are mapped to Drop Precedence 0.

Command Mode
Global Configuration mode.

Example
The following example maps DSCP values 25, 27 and 29 to Drop Precedence 2.

```
switchxxxxxx(config)# qos map dscp-dp 25 27 29 to 2
```

46.32 qos trust (Global)
Use the **qos trust** Global Configuration mode command to configure the system to the basic mode and trust state. Use the **no** form of this command to return to the default configuration.

Syntax
qos trust *{**cos** | **dscp**}*

no qos trust

Parameters
- **cos**— Specifies that ingress packets are classified with packet CoS values. Untagged packets are classified with the default port CoS value.
- **dscp**—Specifies that ingress packets are classified with packet DSCP values.

Default Configuration
CoS is the default trust mode.

Command Mode
Global Configuration mode

User Guidelines
This command can be used only in QoS basic mode.

Packets entering a QoS domain are classified at its edge. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain.

Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When the system is configured with trust DSCP, the traffic is mapped to the queue by the DSCP-queue map.

When the system is configured with trust CoS, the traffic is mapped to the queue by the CoS-queue map.

For an inter-QoS domain boundary, configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different in the QoS domains.

Example
The following example configures the system to the DSCP trust state.

```
switchxxxxxx(config)# qos trust dscp
```

46.33 qos trust (Interface)

Use the **qos trust** Interface Configuration (Ethernet, Port-channel) mode command to enable port trust state while the system is in the basic QoS mode. Use the **no** form of this command to disable the trust state on each port.

Syntax

qos trust

no qos trust

Parameters

N/A

Default Configuration

Each port is enabled while the system is in basic mode.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example configures `fe1/0/1`15 to the default trust state.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# qos trust
```

46.34 qos cos

Use the **qos cos** Interface Configuration (Ethernet, Port-channel) mode command to define the default CoS value of a port. Use the **no** form of this command to restore the default configuration.

Syntax

qos cos *default-cos*

no qos cos

Parameters

default-cos—Specifies the default CoS value (VPT value) of the port. If the port is trusted and the packet is untagged, then the default CoS value become the CoS value. (Range: 0–15)

Default Configuration

The default CoS value of a port is 0.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

Use the default CoS value to assign a CoS value to all untagged packets entering the interface.

Example
The following example defines the port fe1/0/15 default CoS value as 3.

```
switchxxxxxx(config)# interface fe1/0/15
switchxxxxxx(config-if)# qos cos 3
```

46.35 qos dscp-mutation
Use the **qos dscp-mutation** Global Configuration mode command to apply the DSCP Mutation map to system DSCP trusted ports. Use the **no** form of this command to restore the trusted port with no DSCP mutation.

Syntax
qos dscp-mutation

no qos dscp-mutation

Parameters
N/A

Default Configuration
N/A

Command Mode
Global Configuration mode.

User Guidelines
Apply the DSCP-to-DSCP-mutation map to a port at the boundary of a Quality of Service (QoS) administrative domain. If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. Apply the map to ingress and to DSCP-trusted ports only. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress ports. If applying the DSCP mutation map to an untrusted port, to class of service (CoS), or to an IP-precedence trusted port.

Global trust mode must be DSCP or CoS-DSCP. In advanced CoS mode, ports must be trusted.

Example
The following example applies the DSCP Mutation map to system DSCP trusted ports.

```
switchxxxxxx(config)# qos dscp-mutation
```

46.36 qos map dscp-mutation
Use the **qos map dscp-mutation** Global Configuration mode command to configure the DSCP to DSCP Mutation table. Use the **no** form of this command to restore the default configuration.

Syntax
qos map dscp-mutation *in-dscp* to *out-dscp*

no qos map dscp-mutation [*in-dscp*]

Parameters
- **in-dscp**—Specifies up to 8 DSCP values to map, separated by spaces. (Range: 0–63)
- **out-dscp**—Specifies up to 8 DSCP mapped values, separated by spaces. (Range: 0–63)

Default Configuration
The default map is the Null map, which means that each incoming DSCP value is mapped to the same DSCP value.

Command Mode
Global Configuration mode.

User Guidelines
This is the only map that is not globally configured. It is possible to have several maps and assign each one to a different port.

Example
The following example changes DSCP values 1, 2, 4, 5 and 6 to DSCP Mutation Map value 63.

```
switchxxxxxx(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

46.37 show qos map
Use the **show qos map** EXEC mode command to display the various types of QoS mapping.

Syntax
show qos map [**dscp-queue** | **dscp-dp** | **policed-dscp** | **dscp-mutation**]

Parameters
- **dscp-queue**—Displays the DSCP to queue map.
- **dscp-dp**—Displays the DSCP to Drop Precedence map.
- **policed-dscp**—Displays the DSCP to DSCP remark table.
- **dscp-mutation**—Displays the DSCP-DSCP mutation table.

Default Configuration
Display all maps.

Command Mode
EXEC mode

Example
The following example displays the QoS mapping information.

```
switchxxxxxx#  show qos map dscp-queue
Dscp-queue map:

d1   :    d2   0    1    2    3    4    5    6    7    8    9
--   --   --   --   --   --   --   --   --   --   --   --
0    :         01   01   01   01   01   01   01   01   01   01
1    :         01   01   01   01   01   01   01   02   02   02
2    :         02   02   02   02   03   03   03   03   03   03
3    :         04   04   05   05   05   05   05   05   05   05
4    :         06   06   06   06   06   06   06   06   07   07
5    :         07   07   07   07   07   07   08   08   08   08
6    :         08   08   08   08
```

46.38 clear qos statistics
Use the **clear qos statistics** EXEC mode command to clear the QoS statistics counters.

Syntax
clear qos statistics

Parameters
N/A

Default Configuration
N/A

Command Mode
EXEC mode

Example
The following example clears the QoS statistics counters.

```
switchxxxxxx# clear qos statistics
```

46.39 qos statistics policer
Use the **qos statistics policer** Interface Configuration (Ethernet, Port-channel) mode command to enable counting in-profile and out-of-profile. Use the **no** form of this command to disable counting.

This command is relevant only when policers are defined.

Syntax
qos statistics policer *policy-map-name class-map-name*

no qos statistics policer *policy-map-name class-map-name*

Parameters

- **policy-map-name**—Specifies the policy map name.
- **class-map-name**—Specifies the class map name.

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config-if)# qos statistics policer policy1 class1
```

46.40 qos statistics aggregate-policer

Use the **qos statistics aggregate-policer** Global Configuration mode command to enable counting in-profile and out-of-profile. Use the **no** form of this command to disable counting.

Syntax

qos statistics aggregate-policer *aggregate-policer-name*

no qos statistics aggregate-policer *aggregate-policer-name*

Parameters

aggregate-policer-name—Specifies the aggregate policer name.

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Global Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config)# qos statistics aggregate-policer policer1
```

46.41 qos statistics queues

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues. Use the **no** form of this command to disable QoS statistics for output queues.

Syntax

qos statistics queues *set {queue* | ***all}*** *{**dp*** | ***all}*** *{interface* | ***all}***

no qos statistics queues *set*

Parameters

- **set**—Specifies the counter set number.
- **interface**—Specifies the Ethernet port.
- **queue**—Specifies the output queue number.
- **dp**—Specifies the drop precedence. The available values are: **high**, **low**.

Default Configuration

Set 1: All interfaces, all queues, high DP.

Set 2: All interfaces, all queues, low DP.

Command Mode

Global Configuration mode

User Guidelines

There are no user guidelines for this command.

If the queue parameter is all, traffic in stacking and cascading ports is also counted.

Example

The following example enables QoS statistics for output queues for counter set 1.

```
switchxxxxxx(config)# qos statistics queues 1 all all all
```

46.42 show qos statistics

Use the **show qos statistics** EXEC mode command to display Quality of Service statistical information.

Syntax

show qos statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC mode

User Guidelines

Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Use the **qos statistics queues** Global Configuration mode command to enable QoS statistics for output queues.

Example

The following example displays Quality of Service statistical information.

```
switchxxxxxx# show qos statistics
Policers
---------

Interface   Policy map   Class      In-profile       Out-of-profile bytes
                         Map        bytes            --------------------
--------    ----------   -------    -------------    5433
fe1/0/11    Policy1      Class1     7564575          52
fe1/0/11    Policy1      Class2     8759             3214
fe1/0/12    Policy1      Class1     746587458        23
fe1/0/12    Policy1      Class2     5326

Aggregate Policers
------------------

Name        In-profile bytes        Out-of-profile bytes
--------    ----------------        --------------------
Policer1    7985687                 121322

Output Queues
-------------

Interface   Queue       DP          Total packets    %TD packets
---------   -----       --          -------------    -----------
fe1/0/11    2           High        799921           1.2%
fe1/0/12    All         High        5387326          0.2%
```

46.43 security-suite enable

Use the **security-suite enable** Global Configuration mode command to enable the security suite feature. This feature supports protection against various types of attacks.

When this command is used, hardware resources are reserved. These hardware resources are released when the **no security-suite enable** command is entered.

The security-suite feature can be enabled in one of the following ways:

- **Global-rules-only** - This enables the feature globally but per-interface features are not enabled.
- **All** (no keyword) - The feature is enabled globally and per-interface.

Use the **no** form of this command to disable the security suite feature.

When security-suite is enabled, you can specify the types of protection required. The following commands can be used:

- security-suite dos protect
- security-suite dos syn-attack
- security-suite deny martian-addresses
- security-suite deny syn
- security-suite deny icmp
- security-suite deny fragmented
- show security-suite configuration
- security-suite dos protect

Syntax

security-suite enable ***[global-rules-only]***

no security-suite enable

Parameters

global-rules-only—Specifies that all the security suite commands are global commands only (they cannot be applied per-interface). This setting saves space in the Ternary Content Addressable Memory (TCAM). If this keyword is not used, security-suite commands can be used both globally on per-interface.

Default Configuration

The security suite feature is disabled.

If **global-rules-only** is not specified, the default is to enable security-suite globally and per interfaces.

Command Mode

Global Configuration mode

User Guidelines

MAC ACLs must be removed before the security-suite is enabled. The rules can be re-entered after the security-suite is enabled.

If ACLs or policy maps are assigned on interfaces, per interface security-suite rules cannot be enabled.

Examples

Example 1 - The following example enables the security suite feature and specifies that security suite commands are global commands only. When an attempt is made to configure security-suite on a port, it fails.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the
per-interface mode.
```

Example 2 - The following example enables the security suite feature globally and on interfaces. The security-suite command succeeds on the port.

```
switchxxxxxx(config)# security-suite enable
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
switchxxxxxx(config-if)#
```

46.44 security-suite dos protect

Use the **security-suite dos protect** Global Configuration mode command to protect the system from specific well-known Denial of Service (DoS) attacks. There are three types of attacks against which protection can be supplied (see parameters below).

Use the **no** form of this command to disable DoS protection.

Syntax

security-suite dos protect *{**add** attack* | ***remove** attack}*

no security-suite dos protect

Parameters

add/remove *attack*—Specifies the attack type to add/remove. To add an attack is to provide protection against it; to remove the attack is to remove protection.

The possible attack types are:

- **stacheldraht**—Discards TCP packets with source TCP port 16660.
- **invasor-trojan**—Discards TCP packets with destination TCP port 2140 and source TCP port 1024.
- **back-orifice-trojan**—Discards UDP packets with destination UDP port 31337 and source UDP port 1024.

Default Configuration

No protection is configured.

Command Mode

Global Configuration mode

User Guidelines

For this command to work, security-suite enable must be enabled globally.

Example

The following example protects the system from the Invasor Trojan DOS attack.

```
switchxxxxxx(config)# security-suite dos protect add invasor-trojan
```

46.45 security-suite deny martian-addresses

Use the **security-suite deny martian-addresses** Global Configuration mode command to deny packets containing system-reserved IP addresses or user-defined IP addresses.

Syntax

security-suite deny martian-addresses *{**add** {ip-address {mask* | */prefix-length}}* | ***remove*** *{ip-address {mask* | */prefix-length}}* *(*Add/remove user-specified IP addresses)

security-suite deny martian-addresses ***reserved*** *{**add*** | ***remove}*** *(*Add/remove system-reserved IP addresses, see tables below)

no security-suite deny martian-addresses (This command removes addresses reserved by **security-suite deny martian-addresses** *{**add** {ip-address {mask* | */prefix-length}}* | ***remove*** *{ip-address {mask* | */prefix-length}},* and removes all entries added by the user. The user can remove a specific entry by using **remove** *ip-address {mask* | */prefix-length}* parameter.

There is no **no** form of the **security-suite deny martian-addresses** ***reserved*** *{**add*** | ***remove}*** command. Use instead the **security-suite deny martian-addresses reserved** ***remove*** command to remove protection (and free up hardware resources).

Parameters

- **reserved add/remove**—Add or remove the table of reserved addresses below.
- **ip-address**—Adds/discards packets with the specified IP source or destination address.
- **mask**—Specifies the network mask of the IP address.
- **prefix-length**—Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/).
- **reserved**—Discards packets with the source or destination IP address in the block of the reserved (Martian) IP addresses. See the User Guidelines for a list of reserved addresses.

Default Configuration

Martian addresses are allowed.

Command Mode

Global Configuration mode

User Guidelines

For this command to work, security-suite enable must be enabled globally.

security-suite deny martian-addresses *reserved* adds or removes the addresses in the following table:

Address block	Present Use
0.0.0.0/8 (except when 0.0.0.0/32 is the source address)	Addresses in this block refer to source hosts on "this" network.
127.0.0.0/8	This block is assigned for use as the Internet host loopback address.
192.0.2.0/24	This block is assigned as "TEST-NET" for use in documentation and example code.
224.0.0.0/4 as source	This block, formerly known as the Class D address space, is allocated for use in IPv4 multicast address assignments.
240.0.0.0/4 (except when 255.255.255.255/32 is the destination address)	This block, formerly known as the Class E address space, is reserved.

Note that if the reserved addresses are included, individual reserved addresses cannot be removed.

Example

The following example discards all packets with a source or destination address in the block of the reserved IP addresses.

```
switchxxxxxx(config)# security-suite deny martian-addresses reserved
add
```

46.46 security-suite deny syn

Use the **security-suite deny syn** Interface Configuration (Ethernet, Port-channel) mode command to block the creation of TCP connections from a specific interface. This a complete block of these connections.

Use the **no** form of this command to permit creation of TCP connections.

Syntax

security-suite deny syn {***[add*** *{tcp-port* | ***any}*** *{ip-address* | ***any}*** *{mask* | */prefix-length}]* | ***[remove*** *{tcp-port* | ***any}*** *{ip-address* | ***any}*** *{mask* | */prefix-length}]]*

no security-suite deny syn

Parameters

- **ip-address** | **any**—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **mask**— Specifies the network mask of the destination IP address.
- **prefix-length**—Specifies the number of bits that comprise the destination IP address prefix. The prefix length must be preceded by a forward slash (/).
- **tcp-port** | **any**—Specifies the destination TCP port. The possible values are: **http**, **ftp-control**, **ftp-data**, **ssh**, **telnet**, **smtp**, **dns**, **tftp**, **ntp**, **snmp** or **port number**. Use **any** to specify all ports.

Default Configuration

Creation of TCP connections is allowed from all interfaces.

If the **mask** is not specified, it defaults to 255.255.255.255.

If the ***prefix-length*** is not specified, it defaults to 32.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

For this command to work, security-suite enable must be enabled both globally and for interfaces.

The blocking of TCP connection creation from an interface is done by discarding ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses and destination TCP ports.

Example

The following example attempts to block the creation of TCP connections from an interface. It fails because security suite is enabled globally and not per interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny syn add any /32 any
To perform this command, DoS Prevention must be enabled in the
per-interface mode.
```

47 Revision History

Table 3: Revision History Franchise Phase 2.5

Revision	Date	Comments
0.2	August 16, 2010	Updated draft.
0.1	May 18, 2011	Initial draft.

Marvell Semiconductor, Inc.
5488 Marvell Lane
Santa Clara, CA 95054, USA

Tel: 1.408.222.2500
Fax: 1.408.988.8279

www.marvell.com

Marvell. Moving Forward Faster