Franchise Ph. 3.5 CLI Commands

CLI Reference Guide

Document Conventions

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

Document Status

Doc Status:	

Table of Contents

1 Preface

The 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:

- User (Privilege) Levels
- CLI Command Modes
- Starting the CLI
- CLI Command Conventions
- Interface Naming Conventions
- Entering Commands
- IPv6z Address Conventions
- IP Address and OutOfBand Port

User (Privilege) Levels

Users can be created with one of the following user levels:

- Level 1 —Users with this level can only run User EXEC mode commands. Users at this level cannot access the web GUI or commands in the Privileged EXEC mode.
- Level 15 —Users with this level can run all commands. Only users at this level can access the web GUI.

A system administrator (user with level 15) can create passwords that allow a level 1 user to temporarily become a level 15 user.

The passwords for each level are set (by an administrator) using the following command:

```
enable password [level privilege-level]{password|encrypted
encrypted-password}
```

Using these passwords, you can raise your user level by entering the command: enable and the password for level 15. The higher level holds only for the current session.

The **disable** command returns the user to a lower level.

To create a user and assign it a user level, use the **username** command. Only users with command level 15, can create users at this level.

Examples

Create passwords for level 15 (by the administrator):

```
switchxxxxxx#configure
switchxxxxxx<conf># enable password level 15 level15@abc
switchxxxxxx<conf>#
```

Create a user with user level 1:

```
switchxxxxxx#configure
switchxxxxxx<conf> username john password john1234 privilege 1
switchxxxxxx<conf>
```

Switch between Level 1 to Level 15. The user must know the password:

```
switchxxxxxx#
switchxxxxxx# enable
Enter Password: ****** (this is the password for level 15 - level15@abc)
switchxxxxxx#
```

If authentication of passwords is performed on RADIUS or TACACS+ servers, the passwords assigned to user level 15 must be configured on the external server and associated with the $enable15$ user names. See the Authentication, Authorization and Accounting (AAA) Commands chapter for details.

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*

Interface Naming Conventions

Within the CLI, interfaces are denoted by concatenating the following elements:

- **Type of interface**—The following types of interfaces are found on the various types of devices:
  - **GigabitEthernet ports (10/100/1000 bits)**—This can be written as either **GigabitEthernet** or **gi** or **GE.**
  - **TenGigabit thernet ports (10000 bits)**—This can be written as either **TenGigabitEthernet** or **te or xg.**
  - **LAG (Port Channel)**—This can be written as either **Port-Channel** or **po.**
  - **VLAN**—This is written as **VLAN**
  - **Tunnel**—This is written as **tunnel** or **tu**
  - **OOB -** This is written as OutOfBand or **oob**
- Unit Number - Unit in stack. In standalone models this is always 1 (1 by default)
- **Slot Number -** Always 1
- **Interface Number**—Port, LAG, tunnel or VLAN ID

The syntax for this is:

```
{<ethernet-type>[ ][<unit-number>/]<slot-number>/<port-number>}  | {port-channel |
po | ch}[ ]<port-channel-number> |
{tunnel | tu}[ ]<tunnel-number> | vlan[ ]<vlan-id>
```

Sample of these various options are shown in the example below:

```
console(config)#interface GigabitEthernet 1/1/1
console(config)#interface GE 1/1/1
console(config)#interface gi1/1/1
console(config)#interface FastEthernet 1/2/1
console(config)#interface fe1/2/1
console(config)#interface po1
console(config)# interface vlan 1
```

Interface Range

Interfaces may be described on an individual basis or within a range. The interface range command has the following syntax:

```
<interface-range> ::=
{<port-type>[ ][<unit-number>/]<slot-number>/<first-port-number>[ -
<last-port-number]}  |
port-channel[ ]<first-port-channel-number>[ - <last-port-channel-number>] |
tunnel[ ]<first-tunnel-number>[ - <last-tunnel-number>] |
vlan[ ]<first-vlan-id>[ - <last-vlan-id>]
```

A sample of this command is shown in the example below:

```
console#configure
console(config-if)#interface range gi1/1/1-5
```

Interface List

A combination of interface types can be specified in the **interface range** command in the following format:

```
<range-list> ::= <interface-range> | <range-list>, < interface-range>
```

Up to five ranges can be included.

Note. Range lists can contain either ports and port-channels or VLANs. Combinations of port/port-channels and VLANs are not allowed

The space after the comma is optional.

When a range list is defined, a space after the first entry and before the comma (,) must be entered.

A sample of this command is shown in the example below:

```
console#configure
console(config)#interface range gi1/1/1-5 , vlan 1-2
```

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 gi1/1/5**", **show**, **interfaces** and **status** are keywords, **gi** is an argument that specifies the interface type, and **[application-specific]** 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 1.

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 1: 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.

IPv6z Address Conventions

The following describes how to write an IPv6z address, which is a link-local IPv6 address:

The format is: `<ipv6-link-local-address>%<egress-interface>`

where:

egress-interface (also known as zone) = vlan<vlan-id> | po <number> | tunnel <number> | port<number> | 0

If the egress interface is not specified, the default interface is selected. Specifying egress interface = 0 is equal to not defining an egress interface.

The following combinations are possible:

- ipv6_address%egress-interface—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.

IP Address and OutOfBand Port

The switch supports an IP stack on the OutOfBand (OOB) port. This IP stack is separate from the IP stack running on the ASIC ports, and it has a separate routing table.

If the switch supports more than one IP interface, when you specify a remote IP address or a DNS name, you must also specify the IP stack that is being referred to.

To indicate that the OOB IP stack is being specified, add 'oob/' before the remote IP address or the DNS name.

The following examples specify the OOB network::

- ping oob/1.1.1.1
- sntp server oob/sntp-server.company.com
- permit ip-source 2.2.2.0 mask /24 oob (Management ACL)

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, 15)

Default Configuration

The default privilege level is 15.

Command Mode

EXEC mode

Example

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 1.

```
switchxxxxxx# disable 1
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.

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. 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. 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

terminal no 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 not limited, 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 terminal width

Use the **terminal width** EXEC mode command to determine the width of the display for the echo input to CLI sessions. Use **terminal no width** to return to the default.

The command is per session and will not be saved in the configuration database.

Syntax

terminal width *number-of-characters*

terminal no width

Parameters

number-of-characters - Specifies the number of characters to be displayed for the echo output of the CLI commands and the configuration file,'0' means endless number of characters on a screen line. (Range: 0, 70-512)

Default Configuration

The default number of characters is 77.

Command Mode

Privileged EXEC mode

Example

The following example sets the terminal width to 100 characters

```
switchxxxxxx# terminal width 100
```

2.15 terminal prompt

Use the **terminal prompt** EXEC mode command to enable the terminal prompts. Use **terminal no prompt** command to disable the terminal prompts.

The command is per session and will not be saved in the configuration database.

Syntax

terminal prompt

terminal no prompt

Parameters

N/A

Default Configuration

The default configuration is prompts enabled.

Command Mode

Privileged EXEC mode

Example

The following example disables the terminal prompts

```
switchxxxxxx# terminal no prompt
```

2.16 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
```

2.17 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)
```

2.18 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
```

2.19 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           gi1/1/1-39,Po1,Po2,         other        Required
 2    2           gi1/1/1                     dynamicGvrp  Required
 10   v0010       gi1/1/1                     permanent    Not Required
 11   V0011       gi1/1/1,gi1/1/3                 permanent    Required
 20   20          gi1/1/1                     permanent    Required
 30   30          gi1/1/1,gi1/1/3                 permanent    Required
 31   31          gi1/1/1                     permanent    Required
 91   91          gi1/1/1,gi1/1/4                 permanent    Required
 4093 guest-vlan  gi1/1/1,gi1/1/3                 permanent    Guest
switchxxxxxx(config)#
```

2.20 banner exec

Use the **banner exec** Global Configuration mode command to specify and enable a message to be displayed after a successful logon. This banner is applied automatically on all the CLI interfaces: console, Telnet and SSH. 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.
```

2.21 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
```

2.22 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
```

2.23 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
```

2.24 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
```

2.25 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
```

2.26 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.
- 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** 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 $*keyword1* $*keyword2* $*keyword3*

    where $keywordn 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

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 gi1/1/2
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 gi1/1/2
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 gi1/1/2
switchxxxxxx(config-if)#macro apply dup
switchxxxxxx(config-if)#exit
switchxxxxxx(config)#interface gi1/1/3
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)
------------   --------------------------------------------------
gi1/1/2             dup
gi1/1/3             duplex | dup | duplex
---------------------------------------------------------------
switchxxxxxx#configure
switchxxxxxx(config)#interface gi1/1/2
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* **|** ***detailed****]* | ***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.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display description of all macros on present ports. If detailed is not used, only present ports are displayed.

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 gi1/1/2
Interface Macro Description
--------------------------------------------------------------
gi1/1/2 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 logs 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.

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 [[**in** [hhh:mm | mmm] | **at** hh:mm [day month]] | **cancel**] [**slot** *unit-id]*

Parameters

- **in** hhh:mm | mmm - Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
- **at** hh:mm - Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.
- **day** - Number of the day in the range from 1 to 31.
- **month** - Month of the year.
- **cancel** - Cancels a scheduled reload.
- **slot** *unit-id*—Specifies the unit number to be reloaded. (Range: 1–0). If unspecified, reloads all the units.

Default Usage

N/A

Command Mode

Privileged EXEC mode

User Guidelines

The **at** keyword can be used only if the system clock has been set on the device. To schedule reloads across several devices to occur simultaneously, synchronize the time on each device with SNTP.

When you specify the reload time using the **at** keyword, if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

To display information about a scheduled reload, use the **show reload** command.

Examples

Example 1: 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]
```

Example 2: The following example reloads the operating system in 10 minutes on all units.

```
switchxxxxxx# reload in 10
This command will reset the whole system and disconnect your current
session. Reload is scheduled for 11:57:08 UTC Fri Apr 21 2012 (in 10
minutes). Do you want to continue? (y/n) [Y]
```

Example 3: The following example reloads the operating system at 13:00 on all units.

```
switchxxxxxx# reload at 13:00
This command will reset the whole system and disconnect your current
session. Reload is scheduled for 13:00:00 UTC Fri Apr 21 2012 (in 1 hour
and 3 minutes). Do you want to continue? (y/n) [Y]
```

Example 4: The following example cancels a reload.

```
switchxxxxxx# reload cancel
Reload cancelled.
```

4.7 show reload

The **show reload** Privileged EXEC mode command displays reload status of the device.

Syntax

show reload

Parameters

N/A

Default Usage

N/A

Command Mode

Privileged EXEC mode

User Guidelines

You can use the **show reload** command to display a pending software reload. To cancel the reload, use the **reload cancel** privileged EXEC command.

Example

The following example displays that reboot is scheduled for 00:00 on Saturday, April-20.

```
switchxxxxxx# show reload
Reload scheduled for 00:00:00 UTC Sat April 20 (in 3 hours and 12 minutes)
```

4.8 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
```

4.9 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%
```

4.10 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
```

4.11 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
```

4.12 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
```

4.13 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
```

4.14 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.

4.15 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: 1–0)

Command Mode

EXEC mode

Example

4.16 show version

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

Syntax

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

Parameters

- *unit* —Specifies the unit number. (Range: 1–0)

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
```

4.17 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: 1–0)

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
```

4.18 show environment

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

Syntax

show environment {all | fan | temperature {status} | ***stack*** *[switch-number]***}**

Parameters

- **all** —Displays the fan and temperature general status
- **fan** —Displays the fan status
- **temperature status** —Displays the temperature status
- **stack switch-number** —Displays detailed environment status of a stack. If the switch-number is specified, the environment status of the selected device number is displayed. (Range: 1–0)

Command Mode

EXEC mode

User Guidelines

The **fan** and **temperature status** parameters are available only on devices on which FAN and/or temperature sensor are installed.

Fan status can be one of:

- **OK** - The fan/s functions correctly.
- **Failure** - The fan failed.
- **NA** - No fan is installed.
-

Sensor status can be one of:

- **OK** - The sensor/s functions correctly.
- **Failure** - The sensor/s failed.
- **NA** - No sensor is installed.

Example

The following example displays the general environment status of a device or a stack.

```
switchxxxxxx # show environment all
```

```
FAN is OK
TEMPERATURE is OK
```

The following example displays the general FAN status of a device or a stack.

```
switchxxxxxx # show environment fan
FAN is OK
```

The following example displays the detailed temperature status of a device or a stack.

```
switchxxxxxx # show environment temperature status
TEMPERATURE is OK
```

The following example displays the detailed environment status of a stack.

```
switchxxxxxx # show environment stack
Unit           FAN          FAN
               Status       Direction*
---            ---------    -----------------
1              OK           NA
2              Failure      Front-to-Back
3              OK           Back-to-Front
4              NA
5              Not Present
#EDITOR: * FAN Direction column will be printed only in SKUs which support
this feature, or in a stack when one of the units might support this
feature.
Unit           Sensor      Temperature(C/F)
Status
---            ---------   --------------
1              OK          37/99
2              Failure
3              NA
```

4.19 set system

The **set system** Privileged EXEC mode command puts the device into various modes depending on the parameters entered.

Syntax

set system ***openflow*** {***active*** | ***inactive***} ***egress_acl*** {***active*** | ***inactive***}

Parameters

- **openflow {active | inactive}**—Specifies that the Openflow feature is active/inactive.
- **egress_acl {active | inactive}**—Specifies that the Egress ACL feature is active/inactive.

Default Configuration

Supports Egress ACL mode

Command Mode

Privileged EXEC mode

User Guidelines

The system mode is saved in the configuration file header to specify the system mode. It appears even if it specifies the default system mode.

If this command is entered manually, the Startup Configuration file is deleted and the device is rebooted. It is highly recommended to back up the Startup Configuration file before executing this command; otherwise the device is configured in the new system mode with an empty configuration.

If the **system mode** is contained in a configuration file that is downloaded to the device, but the file's system mode matches the current system mode, this information is ignored. Otherwise the following cases occurs:

- If this file is copied manually onto the device (using copy tftp, for example), the operation is aborted, and a message is displayed indicating that the system mode must be changed manually.
- If this file is downloaded during the automatic configuration process, the Startup Configuration file is deleted and the device reboots automatically in the new system mode and the device is configured with an empty configuration.

Examples

Example - The following example configures the device to function with Openflow mode active and Egress_ACL mode inactive.

```
switchxxxxxx# set system openflow active egress-acl inactive
```

4.20 show system mode

The **show system mode** EXEC mode command displays information on features control.

Syntax

show system mode

Parameters

N/A

Default Usage

N/A

Command Mode

EXEC mode

Example

The following example displays system mode information.

```
switchxxxxxx#  show system mode
Feature                     State
```

```
------------------        ---------

Egress_acl:               Active
```

4.21 show system tcam utilization

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

unit-id—Specifies the unit number. (Range: 1–0)

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
```

4.22 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
```

```
System Mode: Router
# Management defaults
Telnet: Enabled (Maximum 4 sessions, shared with SSH)
SSH server: Enabled (Maximum 4 sessions, shared with Telnet)
SCP: Enabled (1 session)
HTTP: Enabled, port 80 (Maximum 11 sessions)
HTTPS: Disabled
SNMP: Enabled.
    User: first
SNMP version: V3
SNMP Local Engine ID: 0000000001
SNMP Notifications: Enabled
SNMP Authentication Notifications: Enabled
Console: Enabled.
Cryptographic keys are generated
HTTPS certificate is generated
Management ACL: No ACL is defined
AAA Telnet authentication login: Local user data base
AAA HTTP authentication login: Local data base
AAA HTTPS authentication login: Local data base
Radius accounting: Disabled
Radius: No server is defined
Tacacs: No server is defined
Syslog: No server is defined
Logging: Enabled
Logging to console: Informational messages
Logging to internal buffer: Informational messages
Logging to file: Error messages
Logging to remote server: Informational messages
Maximum no. of syslog messages: 200
SNTP: supported
SNTP Port No.: 123
SNTP Interface: Enabled
IP Domain Naming System: Enabled
DHCP Server: Enabled
DHCP Auto Configuration: Enabled
DHCP Option 67: Enabled
DHCP Option 82: Disabled

# IPv6 defaults
MLD Version: version 2

# 802.1x defaults
```

```
802.1X is disabled
Mode: Multiple session
Guest VLAN: Not defined
Port Authentication Auto Recovery: Disabled

# Interface defaults in present unit
20 GE regular
2 10G fiberOptics
4 GE combo
Duplex: Full
Negotiation: Enabled
Flow control: Off
Mdix mode: auto
LAGs: No LAG is defined
Storm control: Disabled
Storm control mode: unknown unicast, broadcast, multicast
Port security: Disabled
Port security Auto Recovery: Disabled
LLDP: Enabled
LLDPDU Handeling: Filtering
Jumbo frames: Disabled
Port-Channel Load Balancing: Layer 2,3 & 4

# Bridging defaults
Maximum 16K entries
Aging time: 5 minutes
Loopback Detection: Disabled
Loopback Detection mode: Source MAC Address
Loopback Detection Auto Recovery: Disabled

# Multicast defaults
Multicast filtering: Disabled
IGMP snooping: Disabled
Unregistered Multicast Addresses: disabled
MLD snooping: Disabled
Multicast TV Vlan Interface: disabled

# Port monitoring defaults
Port monitor is not defined
Maximum source port: 8
Maximum destination ports for mirroring: 1

# Spanning tree defaults
Spanning tree is Enabled
Spanning tree mode is Classic
Spanning tree interface: Enabled
Port fast: Disabled
BPDU handling: Flooding
BPDU Guard: Disabled
BPDU Guard Auto Recovery: Disabled
Loopback Guard: Disabled
Loopback Guard Auto Recovery: Disabled

# Vlan defaults
Maximum Vlans: 4094
Default VLAN: Enabled
Default VLAN id: 1
GVRP: Disabled
Port mode: Access
PVID: 1
VLAN membership: 1
PVE: Disabled

# Voice vlan defaults
Voice VLAN: Disabled
Cos: 6 with no remark
OUI table:
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

# Network security defaults
DHCP snooping: Disabled
IP source guard: Disabled
ARP inspection: Disabled
ARP inspection Validation: Disabled

# DOS attacks
Security Suite: Enabled

# IP addressing defaults
No IP interface is defined

# QOS and ACLs defaults
QoS mode is basic
QoS Basic Trust Mode: CoS
QoS Advanced Trust Mode: CoS-DSCP
ACL Auto Recovery: Disabled
Queue default mapping:
cos  qid:
 0    3
 1    1
 2    2
 3    4
 4    5
 5    6
 6    7
```

```
7   8
```

4.23 show services tcp-udp

Use the **show services tcp-udp** Privileged EXEC mode command to display information about the active TCP and UDP services.

Syntax

show services tcp-udp

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

The output does not show sessions where the device is a TCP/UDP client.

Examples

```
switchxxxxxx# show services tcp-udp
Type   Local IP Address Remote IP address   Service Name  State
---------------------- ------------------- ------------- -----------
TCP    All:22                               SSH           LISTEN
TCP    All:23                               Telnet        LISTEN
TCP    All:80                               HTTP          LISTEN
TCP    All:443                              HTTPS         LISTEN
TCP    172.16.1.1:23 172.16.1.18:8789       Telnet        ESTABLISHED
TCP6   All-23                               Telnet        LISTEN
TCP6   fe80::200:b0ff:fe00:0-23             Telnet
       fe80::200:b0ff:fe00:0-8999                         ESTABLISHED
UDP    All:161                              SNMP
UDP6A  ll-161                               SNMP
```

4.24 show tech-support

Use the **show tech-support** EXEC mode command to display system and configuration information that can be provided to the Technical Assistance Center when reporting a problem.

Syntax

show tech-support [***config***] [***memory***]

Parameters

- **memory**—Displays memory and processor state data.
- **config**—Displays switch configuration within the CLI commands supported on the device.

Default Configuration

By default, this command displays the output of technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data.

Command Types

Switch command.

Command Mode

EXEC mode

User Guidelines

Caution: Avoid running multiple **show tech-support** commands on a switch or multiple switches on the network segment. Doing so may cause starvation of some time sensitive protocols, like STP.

The **show tech-support** command may time out if the configuration file output takes longer to display than the configured session time out time. If this happens, enter a **set logout timeout** value of **0** to disable automatic disconnection of idle sessions or enter a longer timeout value.

The **show tech-support** command output is continuous, meaning that it does not display one screen at a time. To interrupt the output, press Esc.

If the user specifies the **memory** keyword, the **show tech-support** command displays the following output:

- Flash info (dir if exists, or flash mapping)
- Output of command **show bootvar**
- Buffers info (like **print os buff**)
- Memory info (like **print os mem**)
- Proc info (like print OS tasks)
- Versions of software components
- Output of command **show cpu utilization**

4.25 show system id

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: 1–0)

Command Mode

EXEC mode

Example

The following example displays the system identity information.

```
switchxxxxxx# show system id
Serial number : 17
```

4.26 service cpu-input-rate

The **show cpu input rate** Global Configuration mode command enables counting the rate of input frames to the CPU in packets per seconds (pps).

Syntax

service cpu-input-rate

Command Mode

Global Configuration mode

Example

The following example displays CPU input rate information.

```
switchxxxxxx(conf)# service cpu-input-rate
```

4.27 show cpu input rate

The **show cpu input rate** EXEC mode command displays the rate of input frames to the CPU in packets per seconds (pps).

Syntax

show cpu input rate

Command Mode

EXEC mode

Example

The following example displays CPU input rate information.

```
switchxxxxxx# show cpu input rate
Input Rate to CPU is 1030 pps.
```

4.28 image description

To define image description, use the **image description** command in Global configuration mode. To remove the description, use the **no** form of the command.

Syntax

image description *image-number description*

no image description *image-number*

Parameters

- *image-number*—Specifies the number of the image: **1** or **2**.
- *description*—Specifies the image description: printable text up to 80 characters.

Default Configuration

No description is defined.

Command Mode

Global Configuration mode

Example

The following example defines description for image 1:

```
switchxxxxxx(config)# image description 1 new-image
```

4.29 show image description

To display the image descriptions, use the **show image description** EXEC mode command.

Syntax

show image description

Command Mode

EXEC mode

Examples

The following example displays the image descriptions:

```
switchxxxxxx# show image description
Image Description
  1   Active-Image
  2   Backup-Image
```

5 Stack Commands

5.1 stack master

Use the **stack master** Global/Interface Configuration mode command to configure a specific unit to be the stack master (forced master).

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**, and the master is selected during the master election process.

Command Mode

Global Configuration mode or Interface Configuration mode

User Guidelines

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

Example

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

```
switchxxxxxx(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, ***unit-id-auto***)

Default Configuration

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
```

```
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] [browser]**

no clock source

Parameters

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

browser—Specifies that if the system clock is not already set (either manually or by SNTP) and a user login to the device using a WEB browser (either via HTTP or HTTPS), the system clock will be set according to the browser's time information.

Default Configuration

There is no external clock source.

If no parameter is specified, SNTP will be configured as the time 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.

The Summer Time taken from the DHCP server has precedence over static SummerTime.

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.

The **no** form of the command clears the dynamic Time Zone and Summer Time from the DHCP server are cleared.

In case of multiple DHCP-enabled interfaces, the following precedence is applied:

- information received from DHCPv6 precedes information received from DHCPv4
- information received from DHCP client running on lower interface precedes information received from DHCP client running on higher interfac

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)
- ***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

aa

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 [**both** | **ipv4** | **ipv6**]

no sntp broadcast client enable

Parameters

both—Specifies the IPv4 and IPv6 SNTP Broadcast clients are enabled. If the parameter is not defined it is the default value.

ipv4—Specifies the IPv4 SNTP Broadcast clients are enabled.

ipv6—Specifies the IPv6 SNTP Broadcast clients are enabled.

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 [**both** | **ipv4** | **ipv6**]

no sntp anycast client enable

Parameters

- **both**—Specifies the IPv4 and IPv6 SNTP Anycast clients are enabled. If the parameter is not defined it is the default value.
- **ipv4**—Specifies the IPv4 SNTP Anycast clients are enabled.
- **ipv6**—Specifies the IPv6 SNTP Anycast clients are enabled.

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 . 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

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 gi1/1/3.

```
switchxxxxxx(config)# sntp client enable gi1/1/3
```

6.13 sntp client enable (Interface)

To enable the SNTP Broadcast and Anycast client on an interface, use the **sntp client enable** Interface Configuration command. Use the **no** form of this command to disable the SNTP client.

This command enables the SNTP Broadcast and Anycast client on an interface. Use the **no** form of this command to disable the SNTP client.

Syntax

sntp client enable

no sntp client enable

Parameters

N/A

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration (Ethernet, Port-channel, VLAN) mode

User Guidelines

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

Example

The following example enables the SNTP broadcast and anycast client on an interface.

```
switchxxxxxx(config-if)# sntp client enable
```

6.14 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
```

6.15 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
```

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

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
```

6.17 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
```

6.18 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
Time from Browser is enabled
```

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

```
switchxxxxxx# show clock detail
 15:22:55 SUN Apr 23 2012
Time source is sntp
Time from Browser is enabled

Time zone (DHCPv4 on VLAN1):
Acronym is RAIN
Offset is UTC+2

Time zone (Static):
Offset is UTC+0

Summertime (DHCPv4 on VLAN1):
Acronym is SUN
Recurring every year.
Begins at first Sunday of Apr at 02:00.
Ends at first Tuesday of Sep at 02:00.
Offset is 60 minutes.

Summertime (Static):
Acronym is GMT
Recurring every year.
Begins at first Sunday of Mar at 10:00.
Ends at first Sunday of Sep at 10:00.
Offset is 60 minutes.

DHCP timezone: Enabled
```

6.19 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
MD5 Authentication Keys
-----------------------------------
2   John123
3   Alice456
-----------------------------------
Authentication is not required for synchronization.
No trusted keys
Unicast Clients: enabled
Unicast Clients Polling: enabled
Server: 1.1.1.121
  Polling: disabled
  Encryption Key: disabled
Server: 3001:1:1::1
  Polling: enabled
  Encryption Key: disabled
Server: dns_server.comapany.com
  Polling: enabled
  Encryption Key: disabled
Broadcast Clients: enabled for IPv4 and IPv6
Anycast Clients: disabled
No Broadcast Interfaces
```

6.20 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: 176.1.1.8
  Source: DHCPv4 on VLAN 1
  Status: Up
  Last response: 19:58:22.289 PDT Feb 19 2005
  Stratum Level: 1
  Offset: 7.33mSec
  Delay: 117.79mSec
Server: dns_server.comapany.com
  Source:  static
  Status: Unknown
  Last response: 12:17.17.987 PDT Feb 19 2005
  Stratum Level: 1
  Offset: 8.98mSec
  Delay: 189.19mSec
Server: 3001:1:1::1
  Source: DHCPv6 on VLAN 2
  Status: Unknown
  Last response:
  Offset: mSec
  Delay: mSec
Server: dns1.company.com
  Source: DHCPv6 on VLAN 20
  Status: Unknown
  Last response:
  Offset: mSec
  Delay: mSec

Anycast servers:
Server: 176.1.11.8
  Interface:  VLAN 112
  Status: Up
  Last response: 9:53:21.789 PDT Feb 19 2005
  Stratum Level: 10
  Offset: 9.98mSec
  Delay: 289.19mSec

Broadcast servers:
Server: 3001:1::12
  Interface:  VLAN 101
  Last response: 9:53:21.789 PDT Feb 19 2005
  Stratum Level: 255
```

7 Configuration and Image File Commands

7.1 copy

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

Syntax

copy *source-url destination-url*

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).
- **"Flash://"** —The source or destination URL scheme that specifies the access method to the local flash memory. It stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-conig).

The following table displays the URL options.

Source and/or Destination URL	Source or Destination
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.
scp	Source or destination URL for a Secure Copy Protocol (SCP) network server. The syntax for this alias is: **scp://**[*username***:***password@*]*host***/**[*directory*]**/***filename*. The host can be either the IP address or hostname. The default on the switch is SSH authentication by password with username and password anonymous. The SSH authentication parameters can be reconfigured to match the SSH/SCP server's parameters.
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.

Source and/or Destination URL	Source or Destination
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.
unit://*member*/**backup-config**	Backup configuration file on one of the units.
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.
unit://*member*/**localization**	The secondary language file on one of the units. To copy to all units, specify * in the member field. Example: **copy tftp://10.5.234.203/french.txt unit:**//*/**localization.**
	Specifies the SYSLOG file.
Word<1-128>	Name of file (e.g. backup-config).

Default Configuration

Sensitive data is excluded if no method was specified

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.
- **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.

SCP Copy Authentication Options

The following options are possible for using the SCP copy feature:

- **scp://***host/[directory]***/***filename*

  In this option, the SSH authentication method (either by password or by key) and the credentials are specified by the CLI commands for ip ssh client (**ip ssh-client authentication**, **ip ssh-client key-type or ip ssh-client password/username**, and also the server authentication configuration commands)**,**.

- **scp://***username***:***password@.host/[directory]***/***filename*..

  This option specifies SSH authentication by password, and the user name and password for this specific SCP session (one-time only).

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
```

Example 4 - Copy file1 from SCP server to startup config

The following example copies file1 to the Startup Configuration file. The username and password used for SCP session authentication are: jeff and admin1. The IP address of the server containing file1 is 102.1.2.2.

```
switchxxxxxx# copy scp://jeff:admin1@102.1.2.2/file1 startup-config
```

7.2 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
```

7.3 write

Use the **write** Privileged EXEC mode command to save the running configuration to the startup configuration file.

Syntax

write [memory]

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following example shows how to overwrite the startup-config file with the running-config file with the write command.

```
switchxxxxxx# write
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
```

7.4 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)

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-conig).

The following table displays keywords and URL prefixes:

URL	
startup-config	Startup configuration file.
WORD	Name of file (e.g. backup-config).

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

mirror-config, *.sys, ***.prv**, **image-1** and **image-2** files cannot be deleted.

Example

The following example deletes the file called 'backup-config' from the flash memory.

```
switchxxxxxx# delete flash://backup-config
Delete flash:backup-config? [confirm]
```

7.5 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
---------   ----------  ---------- ---------    ---------
```

```
backup-config  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
mirror-config  rw       524288     104          01-Jan-2010 05:35:04
dhcpsn.prv     --          262144     --         01-Jan-2010 05:25:07
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
```

7.6 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).

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-conig).

The following table displays options for the URL parameter:

Keyword	Source or Destination
running-config	Current running configuration file.
startup-config	Startup configuration file.
mirror-config	Mirrored configuration file.
WORD	Name of file (e.g. backup-config).

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 gi1/1/1-48
speed 1000
exit
no lldp run
line console
exec-timeout 0
```

7.7 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)

"Flash://" is the source or destination URL scheme that specifies the access method to the local flash memory. It simply stands for the root directory of the local flash. It is the default scheme for a URL that does not explicitly contain a scheme/access method (e.g. for copying the running configuration file, the user may either use flash://running-config or just running-conig).

The following table displays options for the URL parameter:

Keyword	Source or Destination
WORD<1-128>	Name of file (e.g. backup-config)..

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

mirror-config, *.sys and ***.prv** files cannot be renamed.

Example

The following example renames the configuration backup file.

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

7.8 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.
- **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 (if the switch parameter is omitted, the active system image file that will be loaded by the device at startup will be set only for the master unit) .

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
```

7.9 show running-config

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

show running-config [***interface*** *interface-id-list* **|** ***detailed*** | ***brief***]

Parameters

- ***interface*** *interface-id-list*—Specifies a list of interface IDs. The interface IDs can be one of the following types: Ethernet port, port-channel or VLAN.
- **detailed**—Displays configuration with SSL and SSH keys.
- **brief**—Displays configuration without SSL and SSH keys.

Default Configuration

All interfaces are displayed. If *detailed* or *brief* is not specified, the default is *detailed*.

Command Mode

Privileged EXEC mode

Example

The following example displays the running configuration file contents.

```
switchxxxxxx# show running-config
config-file-header
SG500X-SA
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
no spanning-tree
interface range gi1/1/1-48
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#
```

7.10 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
config-file-header
SG500X-SA
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
no spanning-tree
interface range gi1/1/1-48
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#
```

7.11 show bootvar

Use the **show bootvar** EXEC mode command to display the active system image file that was loaded by the device at startup, and to display the system image file that will be loaded after rebooting the switch.

Syntax

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

Parameters

unit-id—Specifies the unit number. Range 1-0

Command Mode

EXEC mode

Example

The following example displays the active system image file that was loaded by the device at startup and the system image file that will be loaded after rebooting the switch.

```
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.
```

7.12 service mirror-configuration

Use the **service mirror-configuration** Global Configuration mode command to enable the mirror-configuration service. Use **no service mirror-configuration** command to disable the service.

Syntax

service mirror-configuration

no service mirror-configuration

Parameters

- There are no parameters for this command

Default Configuration

The default configuration is mirror-configuration service enabled.

Command Mode

Global Configuration mode

User Guidelines

The mirror-configuration service automatically keeps a copy of the last known stable configuration (startup configuration that wasn't modified for 24H). The mirror-configuration file is not deleted when restoring to factory default.

When this service is disabled, the mirror-configuration file is not created and if such file already exists, it is deleted.

Note that enabling the service doesn't implicitly creates a mirror-configuration file.

Examples

1. The following example disables the mirror-configuration service

no service mirror-configuration

This operation will delete the mirror-config file if exists. Do you want to continue? (Y/N) [N]

2. The following example enables the mirror-configuration service

service mirror-configuration

Service is enabled.

Note that the running-configuration must be first copied to the startup-configuration in order to initiate backing up the startup-config to the mirror-config.

7.13 show mirror-configuration service

Use the **show mirror-configuration service** EXEC mode command to display the mirror-configuration service status set by service mirror-configuration.

Syntax

show mirror-configuration service

Command Mode

EXEC mode

Example

The following example displays the status of the mirror-configuration service

```
show mirror-configuration service

Mirror-configuration service is enabled
```

8 Auto-Update and Auto-Configuration

8.1 boot host auto-config

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

Syntax

boot host auto-config [**tftp** | **scp** | **auto** [*extension*]]

no boot host auto-config

Parameters

- **tftp**- Only the TFTP protocol is used by auto-configuration.
- **scp**- Only the SCP protocol is used by auto-configuration.
- **auto**-(Default) Auto-configuration uses the TFTP or SCP protocol depending on the configuration file's extension. If this option is selected, the extension parameter may be specified or, if not, the default extension is used.
- **extension**- The SCP file extension. When no value is specified, 'scp' is used. (Range: 0–128)

Default Configuration

The auto option is the default.

Command Mode

Global Configuration mode

Default Configuration

Enabled by default.

Examples:

Example 1. The following example specifies the auto mode and specifies "scon" as the SCP extension:

```
boot host auto-config auto scon
```

Example 2. The following example specifies the auto mode and does not provide an SCP extension. In this case "scp" is used.

```
boot host auto-config auto
```

Example 3. The following example specifies that only the SCP protocol will be used:

```
boot host auto-config scp
```

8.2 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
```

8.3 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.

Example

```
switchxxxxxx(conf)# boot host dhcp
```

8.4 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
```

8.5 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: enabled
Download Protocol Mode is SCP
```

```
SCP extension is scp
Next Boot Config Download via DHCP: default
Auto Config
-----------
Config Download via DHCP: enable
Next Boot Config Download via DHCP: force
Auto Config State: Finished
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
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
```

8.6 ip dhcp tftp-server ip address

Use the **ip dhcp tftp-server ip address** Global Configuration mode command to set the TFTP or SCP 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 the command to return to default.

Syntax

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

no ip dhcp tftp-server ip address

Parameters

ip-addr—IPv4 Address or IPv6 Address or DNS name of TFTPor SCP server.

Default Configuration

No IP address

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server. It can also be an SCP server.

Examples

Example 1. The example specifies the IPv4 address of TFTP server:

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

Example 2. The example specifies the IPv6 address of TFTP server:

```
switchxxxxxx(conf)# ip dhcp tftp-server ip address 3000:1::12
```

Example 3. The example specifies the IPv6 address of TFTP server:

```
switchxxxxxx(conf)# ip dhcp tftp-server ip address tftp-server.company.com
```

8.7 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 or SCPserver 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 the server

Default Configuration

No file name

Command Mode

Global Configuration mode

Examples

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

8.8 show ip dhcp tftp-server

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

Syntax

show ip dhcp tftp-server

Parameters

N/A

Default Configuration

N/A

Command Mode

EXEC

Example

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

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 gi1/1/1 and gi1/1/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit gi1/1/1
switchxxxxxx(config-macl)# permit gi1/1/9
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 `gi1/1/1 and 9`, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny gi1/1/1
switchxxxxxx(config-macl)# deny gi1/1/9
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***l***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 {**console-only** | *name*}

no management access-class

Parameters

- **console-only**—Specifies that the device can be managed only from the console.
- **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
```

```
m1
--
deny service telnet
permit gi1/1/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

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 server

Use the **snmp-server server** Global Configuration mode command to enable the device to be configured by the SNMP protocol. Use the **no** form of this command to disable this function.

Syntax

snmp-server server

no snmp-server server

Parameters

N/A

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

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

10.2 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]*

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.

Default Configuration

No community is defined

Command Mode

Global Configuration mode

User Guidelines

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),

Example

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
```

10.3 snmp-server community-group

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. This command configures both SNMP v1 and v2.

Syntax

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

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.
- **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

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.

Example

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
```

10.4 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
```

10.5 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
```

10.6 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
```

10.7 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.

10.8 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. Use the **encrypted** form of this command to enter the authentication and privacy passwords in encrypted form (see SSD).

Syntax

snmp-server user *username groupname {**v1** |* ***v2c*** *|* *[**remote** host]* ***v3****[**auth** {* ***md5*** *|* ***sha****}* *auth-password [**priv** priv-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).
- **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*—IP address (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..
- **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.
- **priv-password**—Specifies the privacy password (The encryption algorithm used is data encryption standard - DES). Range: Up to 64 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
```

10.9 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

Example

The following examples displays the configured SNMP users

```
switchxxxxxx#show snmp users
User name                 : u1rem
  Group name                : group1
  Authentication Algorithm : None
  Privacy Algorithm         : None
  Remote                  :11223344556677
  Auth Password           :
  Priv Password           :

User name                 : qqq
  Group name                : www
  Authentication Algorithm : MD5
  Privacy Algorithm         : None
  Remote                    :
  Auth Password           : helloworld1234567890987665
  Priv Password           :

User name                    : hello
  Group name                   : world
  Authentication Algorithm     : MD5
  Privacy Algorithm          : DES
  Remote                     :
  Auth Password (encrypted): Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLRdAgOE6XQKTC
                             qMlrnpWuHraRlZj
  Priv Password (encrypted) : kN1ZHzSLo6WWxlkuZVzhLOo1gI5waaNf7Vq6yLBpJdS4N68tL
                             1tbTRSz2H4c4Q4o

User name                    : u1noAuth
  Group name                 : group1
  Authentication Algorithm   : None
  Privacy Algorithm          : None
  Remote                     :
  Auth Password (encrypted):
  Priv Password (encrypted) :

User name                    : u1OnlyAuth
  Group name                 : group1
  Authentication Algorithm   : SHA
  Privacy Algorithm          : None
  Remote                     :
  Auth Password (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
  Priv Password (encrypted) :
```

10.10 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
```

10.11 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
```

10.12 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 list (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 and snmp-server group to create a user or a group.

Example

The following defines a host at the IP address displayed.

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

10.13 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:

To configure the engine ID:

- For standalone devices, enter the default or configure it explicitly. In the latter caseverify that it is unique within the administrative domain.
- For stackable systems, configure a non-default 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
```

10.14 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.

10.15 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
```

10.16 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
```

10.17 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
```

10.18 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
```

10.19 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
```

10.20 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
```

10.21 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

Keys and Certificates

The device automatically generates default RSA/DSA keys and certificates at following times:

- When the device is booted following a software upgrade.
- When the device is booted with an empty configuration.
- When user-defined keys/certificates are deleted.

Some commands in this section are used to generate user-defined RSA/DSA keys and certificates that replace the default keys and are used by SSL and SSH server commands. Other commands can be used to import these keys from an external source.

These keys and certificates are stored in the configuration files.

Table 2 describes when these keys/certificates are displayed..

Table 2: Keys Displayed with Show Commands

File Type Being Displayed.	What is Displayed in a Show Command Without Detailed.	What is Displayed in a Show Command With Detailed.
Startup Config	Only user-defined keys/certificates.	Option is not supported.
Running Config	Keys are not displayed.	All keys (default and user-defined)
Text-based CLI (local backup config. file, mirror config. file or remote backup config. file)	Keys are displayed as they were copied. There is no distinction here between default and user-defined keys.	Option is not supported.

Table 3 describes how keys/certificates can be copied from one type of configuration file to another (using the copy command)..

Table 3: Copying Keys/Certificates

Destination File Type.	Copy from Running Config..	Copy from Startup Config..	Copy from Remote/Local Backup Config. File or Mirror Config. File.
Startup Config.	All keys/certificates are copied (but only user-defined ones can be displayed	Option is not supported.	All keys/certificates present in this file are copied.[1,2]
Running Config	N/A	Only user defined.	All keys/certificates present in this file are copied.[2]
Text-based CLI (local backup config. file, mirror config. file or remote backup config. file)	All keys (default and user)	Only user defined.	All keys/certificates present in this file are copied.[2]

[1] If the Running Configuration file on the device contains default keys (not user-defined ones), the same default keys remain after reboot.

[2] In a text-based configuration file, there is no distinction between automatically-defined, default keys and user-defined keys.

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

The application creates a default key automatically.

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 default or user defined, a warning is displayed with a prompt to replace the existing keys with new keys.

Not relevant before SSD

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).

See Keys and Certificates for information on how to display and copy this key pair.

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

The application creates a default key automatically.

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.

See Keys and Certificates for information on how to display and copy this key pair.

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 crypto key import

The **crypto key import** Global Configuration mode command imports the DSA/RSA key pair.

Use the no form of the command to remove the user key and generate a new default in its place.

Syntax

crypto key import {dsa | rsa}

Parameters

N/A

Default Configuration

DSA and RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

DSA/RSA keys are imported in pairs - one public DSA/RSA key and one private DSA/RSA key.

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

This command is saved in the Running Configuration file.

Example

Example 1 - Import plaintext key

The following example imports RSA key pairs where a RSA key already exists.

```
switchxxxxxx(config)# crypto key import rsa
Replace Existing RSA Key [y/n]? Y
-----BEGIN RSA PRIVATE KEY-----
MIICWQIBAAKBgQDM3fV+7nopIQ5l2sZU8gkekCzwbw0MiQF2pnarRA+IoKcs/DReyT21NU
podlDmMltefzVBmmiVo8skggfcHVxz3oPsgV9WRs9sxFvPbh2m5aY9VUtSVDLmcIp0MK6L
```

```
kopUPrOPeCm6EuEwmivsCMAC7l4GsiLYi7AxUm5qTkzT3wIBIwKBgAu06XT3rzWM3EBVpO
7pQlmElNqKAL7jQemF2uU3FtSbd0RmLuDYTKtE364ypYl/OGvMwTby4Wei9apQkrwe71b5
08eYGCr80QrPWWUE/6FeMDqnJQeZJ8lWHSw5qwAut+wOJ9yHyAQTG2pPas6lM2VYP19HMb
YwBmB3H47zjjfrAkEA8CYFRVHNLWpZ9wEXSGTJe4QIdk8w2SUBNTxrsqrzylo89yuyV/K8
qzvPuXO0rondozPEXd8iBqDir+qLI6Nv9wJBANpjwlZmmNEa1aC+UE4/VXnWMnH0HILVod
hPgozTFJaddE/OSdgKthlFnHLrFw8yt8LVPvZdwjyftn3bmYRwkVkCQHSkwLtE/UHx0+0A
h6bR3jSt2Dl269cvOxnbhMR+63DqAFrMFMuhyVp8IxDvDp3rMSNiSW9sYPvnvo/1lAn+7T
0CQBj1dUuz9DUno2LT6+uvd3ujc3q80A7z1/t2zRdolKN/tYV2qVqE4Zx8++/gWmgjDa/d
209bLCQvgpIKd/Hg+qsCQC3KSMwNTQ11Slsf/iA0QkMrunMsBha59wo+tMfdk3/kZkTdQT
knkRQxydFB7pQBojzbqfYL5Zl/R5HR+2r38Tc=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMzd9X7ueikhDmXaxlTyCR6QLPBvDQyJAXamdqtED4igpyz8NF7JPbU1Smh2UO
YyW15/NUGaaJWjyySCB9wdXHPeg+yBX1ZGz2zEW89uHablpj1VS1JUMuZwinQwrouSilQ+
s494KboS4TCaK+wIwALuXgayItiLsDFSbmpOTNPfAgEj
-----END RSA PUBLIC KEY-----
.
```

Example 2 - Import encrypted key

```
encrypted crypto key import rsa

---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----

Comment: RSA Private Key

84et9C2XUfcRlpemuGINAygnLwfkKJcDM6m2OReALHScqqLhi0wMSSYNlT1IWFZP1kEVHH

Fpt1aECZi7HfGLcp1pMZwjn1+HaXBtQjPDiEtbpScXqrg6ml1/OEnwpFK2TrmUy0Iifwk8

E/mMfX3i/2rRZLkEBea5jrA6Q62gl5naRw1ZkOges+GNeibtvZYSk1jzr56LUr6fT7Xu5i

KMcU2b2NsuSD5yW8R/x0CW2elqDDz/biA2gSgd6FfnW2HV48bTC55eCKrsId2MmjbExUdz

+RQRhzjcGMBYp6HzkD66z8HmShOU+hKd7M1K9U4Sr+Pr1vyWUJlEkOgz9O6aZoIGp4tgm4

VDy/K/G/sI5nVL0+bR8LFUXUO/U5hohBcyRUFO2fHYKZrhTiPT5Rw+PHt6/+EXKG9E+TRs

lUADMltCRvs+lsB33IBdvoRDdl98YaA2htZay1TkbMqCUBdfl0+74UOqa/b+bp67wCYKe9

yen418MaYKtcHJBQmF7sUQZQGP34VPmOMyZzon68S/ZoT77cy0ihRZx9wcI1yYhJnDiYxP

dgXHYhW6kCTcTj6LrUSQuxCJ9su89ZIWNn5OwdgonLSpvfnabv2GHmmelaveL7JJ/7UcfO

61q5D4PJ67Vk2xL7PqyHXN931rseTzPuJplkSLCFZ5uqTMbWWyQEKmHDlOx35vlGou5tky

9LgIwG4d+9edctZZaggeq5cgjnsZWJgUoB4Bn4hIreyOdHDiFUPPRxkoyhGOGnJuvxC9T9

K6BF1wBTdDQS+Gu47/0/gRoD/50q4sGkzqHsRJJ53WOT0Q1bHMTMLPpwn2nXzvfGxWL/bu

QhZZSqRonG6MX1cP7KT7i4TPq2w2k3TGtNBnVYHx6OoNcaTHmg1N2s5OgRsyXD9tF++6nY

RfMN8CsV+9jQKQP7ZaGc8Ju+d72jvSwppSr032HY+IpzZ4ujkK+/X5oawZL5NnkaEQTQKX
```

```
RSL55S4O5NPOjS/pC9hg7GaVjoY2mQ7HDpSUBeTIDTlvOwC2kskA9C6aF/Axj2dXLweQd5

lxk7m0/mMNaiJsNk6y33LcuKjIxpNNjK9n9KzRPkGNMFObprfenWKteDftjQ==

---- END SSH2 PRIVATE KEY ----

---- BEGIN SSH2 PUBLIC KEY ----

Comment: RSA Public Key

AAAAB3NzaC1yc2EAAAABIwAAAIEAvRHsKry6NKMKymb+yWEp9042vupLvYVq3ngt1sB9JH

OcdK/2nw7lCQguy1mLsX8/bKMXYSk/3aBEvaoJQ82+r/nRf0y3HTy4Wp9zV0SiVC8jLD+7

7t0aHejzfUhr0FRhWWcLnvYwr+nmrYDpS6FADMC2hVA85KZRye9ifxT7otE=

---- END SSH2 PUBLIC KEY ----
```

11.4 show crypto key

The **show crypto key** Privileged EXEC mode command displays the device’s SSH public keys for both default and user-defined keys.

Syntax

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

Parameters

- **mypubkey**—Displays only the public key.
- **rsa**—Displays the RSA key.
- **dsa**—Displays the DSA key.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

See Keys and Certificates for information on how to display and copy this key pair.

Example

The following example displays the SSH public DSA keys on the device.

```
switchxxxxxx# show crypto key mypubkey dsa
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzN31fu56KSEOZdrGVPIJHpAs8G8NDIkB
dqZ2q0QPiKCnLPw0Xsk9tTVKaHZQ5jJbXn81QZpolaPLJIIH3B1cc96D7IFf
VkbPbMRbz24dpuWmPVVLUlQy5nCKdDCui5KKVD6zj3gpuhLhMJor7AjAAu5e
BrIi2IuwMVJuak5M098=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 6f:93:ca:01:89:6a:de:6e:ee:c5:18:82:b2:10:bc:1e
```

11.5 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]] [****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)

  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 **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

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 activate one of them.

See Keys and Certificates for information on how to display and copy this key pair.

Erasing the startup configuration or returning to factory defaults automatically deletes the default keys and they are recreated during device initialization.

Example

The following example generates a self-signed certificate for HTTPS whose length is 2048 bytes.

```
switchxxxxxx(config)# crypto certificate 1 generate key-generate 2048
```

11.6 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 generate Global 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-----
```

11.7 crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the RSA key-pair can also be imported.

Use the no form of the command to delete the user-defined keys and certificate.

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 only the certificate is imported, and the public key found in the certificate does not match the device's SSL RSA key, the command fails. If both the public key and the certificate are imported, and the public key found in the certificate does not match the imported RSA key, the command fails.

This command is saved in the Running configuration file.

See Keys and Certificates for information on how to display and copy this key pair.

Examples

Example 1 - The following example imports a certificate signed by the Certification Authority for HTTPS.

```
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
```

Example 2: The following example imports a certificate signed by the Certification Authority for HTTPS, and the RSA key-pair.

```
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 RSA PRIVATE KEY-----
ACnrqImEGlXkwxBuZUlAO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLUlJujM9p1IXFpMk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11EoqzpCq5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENYl7qsZ
MWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWWc0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOuIQaMnhYf+RyPXhPOQs01PpIPHKBGTi6pj39XMviyRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSLhjApf5iIQr1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
ql7yZnBeRS0zrUDgHLLRfzwjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFBYNmbzHc7a+7043wfVmH+QOXf
```

```
TbnRDhIMVrZJGbzl1c9IzGky1l21Xmicy0/nwsXDAgEj
-----END RSA PUBLIC KEY-----
-----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
```

Example 3 - Import certificate with encrypted key

```
encrypted crypto certificate 1 import

-----BEGIN RSA ENCRYPTED PRIVATE KEY-----

wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ

AdQwgWM5mnjUhUaJ1MM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6Pxlv6cKvYYzHg43Unm

CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6

GD/crN28vTLGf/NpyKoOhdAMRuwEQoapMo0Py2Cvy+sqLiv4ZKck1FPlsVFV7X7sh+zVa3

We84pmzyjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJJYrdGKGybqD0o3tD/ioUQ3UJgxDbGYw

aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4HDa6UDN6aoUBalUhqjT+REwWO

DXpJmvmX4T/u5W4DPvELqTHyETxgQKNErlO7gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz

XeoDojSe6OYOQww2R0nAqnZsZPgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ

FkPFNAKvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP

CZM927oxkb41g+U5oYQxGhMK7OEzTmfS1FdLOmfqv0DHZNR4lt4KgqcSjSWPQeYSzB+4PW

Qmy4fTF4wQdvCLy+WlvEP1jWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q

zZFRmDMHPtey9ALO2alpwjpHOPbJKiCMdjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA

J0sxrvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgYWb3V5SI8D8kRejqBM9eaCyJsvLF

+yAI5xABZdTPqz0l7FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
```

```
Vf8jpTLMWFgVF9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRxLAHkifD7ZHrE7udOmTiP9
W3PqtJzbtjjvMjm5/C+hoC6oLNP6qp0TEn78EdfaHpMMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzEeWjdz55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPgWeDHw3q5QkaqInzz1h7j2+A++mwCsHui1BhpFNFY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMTOeO+QSbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCCAYUCEFCcI4/dhLsUhTWxOwbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxEDAOBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHhcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygJor5v2FOCvMR5aN3PnkWhbBXyzniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP
PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iar1+m66RyehO8E2/PvPdU7G/qHDVQcxM5
475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBOknTzas7HniIHMPeC5yC0
2rd7c+zqQOe1e4CpEvV1OC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE
dkB/761PpeKkUtgyPHfTzfSMcJdBOPPnpQcqbxCFh9QSNa4ENSXqC5pND02RHXFx
wS1XJGrhMUoNGz1BY5DJWw==
-----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
```

Example 3 - Import certificate with encrypted key

```
encrypted crypto certificate 1 import
```

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
AdQwgWM5mnjUhUaJ1MM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6Pxlv6cKvYYzHg43Unm
CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRuwEQoapMo0Py2Cvy+sqLiv4ZKck1FPlsVFV7X7sh+zVa3
We84pmzyjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJJYrdGKGybqD0o3tD/ioUQ3UJgxDbGYw
aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4HDa6UDN6aoUBalUhqjT+REwWO
DXpJmvmX4T/u5W4DPvELqTHyETxgQKNErlO7gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6OYOQww2R0nAqnZsZPgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkPFNAKvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP
CZM927oxkb41g+U5oYQxGhMK7OEzTmfS1FdLOmfqv0DHZNR4lt4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvEP1jWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwjpHOPbJKiCMdjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0sxrvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgYWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABZdTPqz0l7FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jpTLMWFgVF9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRxLAHkifD7ZHrE7udOmTiP9
W3PqtJzbtjjvMjm5/C+hoC6oLNP6qp0TEn78EdfaHpMMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzEeWjdz55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPgWeDHw3q5QkaqInzz1h7j2+A++mwCsHui1BhpFNFY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMTOeO+QSbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCCAYUCEFCcI4/dhLsUhTWxOwbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxEDAOBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHhcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygJor5v2FOCvMR5aN3PnkWhbBXyzniTl
```

```
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP

PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iar1+m66RyehO8E2/PvPdU7G/qHDVQcxM5

475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBOknTzas7HniIHMPeC5yC0

2rd7c+zqQOe1e4CpEvV1OC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE

dkB/761PpeKkUtgyPHfTzfSMcJdBOPPnpQcqbxCFh9QSNa4ENSXqC5pND02RHXFx

wS1XJGrhMUoNGz1BY5DJWw==

-----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
```

11.8 show crypto certificate

The **show crypto certificate** Privileged EXEC mode command displays the device SSL certificates and key-pair for both default and user defined keys.

Syntax

show crypto certificate [mycertificate] [*number*]

Parameters

- **number**—Specifies the certificate number. (Range: 1,2)

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
Certificate 1:
Certificate Source: Default
-----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
Fingerprint: DC789788 DC88A988 127897BC BB789788

Certificate 2:
Certificate Source: User-Defined
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----
Issued by: www.verisign.com
Valid from: 8/9/2004 to 8/9/2005
Subject: CN= router.gm.com, 0= General Motors, C= US
Fingerprint: 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
```

12.9 ssl version

Use the **ssl version** Global Configuration command to define the version of the supported SSL.

Use the no form to return to the default.

Syntax

ssl version {v2&v3 | v3}

no ssl version

Parameters

- **v2&v3**—SSLv2 and SSLv3 are supported after reboot.
- **v3** —Only versions starting with SSLv3 are supported after reboot.

Defaults

v3

Command Modes

```
Global configuration
```

Examples

```
switchxxxxxx#ssl version v3&v3
```

12.10 show ssl version

Use the **show ssl versions** Privilege EXEC command to display the SSL supported version.

Syntax

show ssl version

Parameters

N/A

Defaults

N/A

Command Modes

Privilege EXEC

Examples

```
switchxxxxxx#show ssl version
Current supported version: SSLv2 and SSLv3
```

13 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 as a Telnet server that accepts connection requests from remote Telnet clients. Remote Telnet clients can configure the device through the Telnet connections.

Use the no form of this command to disable the Telnet server functionality on the device.

Syntax

ip telnet server

no ip telnet server

Default Configuration

The Telnet server functionality on the device is Enabled by default

Command Mode

Global Configuration mode

User Guidelines

The device can be enabled to accept connection requests from both remote SSH and Telnet clients. It is recommended that the remote client connects to the device using SSH (as opposed to Telnet), since SSH is a secure protocol and Telnet is not. To enable the device to be a SSH server, use the **ip ssh server** 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 an SSH server and so to accept connection requests from remote SSH clients. Remote SSH clients can manage the device through the SSH connection.

Use the **no** form of this command to disable the SSH server functionality from the device.

Syntax

ip ssh server

no ip ssh server

Default Configuration

The SSH server functionality is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The device as a SSH server generates the encryption keys automatically.

To generate new 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 to be an SSH server.

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

13.3 ip ssh port

The **ip ssh port** Global Configuration mode command specifies the TCP 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 TCP port number to be used by the SSH server. (Range: 1–65535)

Default Configuration

The default TCP port number is 22.

Command Mode

Global Configuration mode

Example

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

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

13.4 ip ssh password-auth

Use the **ip ssh password-auth** Global Configuration mode command to enable password authentication of incoming SSH sessions.

Use the **no** form of this command to disable this function.

Syntax

ip ssh password-auth

no ip ssh password-auth

Default Configuration

Password authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables password key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

Example

The following example enables password authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh password-auth
```

13.5 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 [**auto-login**]

no ip ssh pubkey-auth

Parameters

- **auto-login**—Specifies that the device management AAA authentication (CLI login) is not needed. By default, the login is required after the SSH authentication.

Default Configuration

Public Key authentication of incoming SSH sessions is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables public key authentication by a local SSH server of remote SSH clients.

The local SSH server advertises all enabled SSH authentication methods and remote SSH clients are responsible for choosing one of them.

After a remote SSH client is successfully authenticated by public key, the client must still be AAA-authenticated to gain management access to the device, except if the auto-login parameter was specified.

.

If no SSH authentication method is enabled, remote SSH clients must still be AAA-authenticated before being granted management access to the device.

If the **auto-login** keyword is specified for SSH authentication by public key, then management access is granted if SSH authentication succeeds and the name of SSH used is found in the local user database. The device management AAA authentication is transparent to the user. If the user name is not in the local user database, then the user receives a warning message, and the user will need to passs the device management AAA authentication independent to the SSH authentication.

if the **auto-login** keyword is not specified, management access is granted only if the user engages and passes both SSH authentication and device management AAA authentication independently.If no SSH authentication method is enabled then management access is granted only if the user is AAA authenticated by the device management. No SSH authentication method means SSH is enabled but neither SSH authentication by public key nor password is enabled.

Example

The following example enables authentication of the SSH client.

```
switchxxxxxx(config)# ip ssh pubkey-auth
```

13.6 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 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
```

13.7 user-key

The **user-key** SSH Public Key-string Configuration mode command associates a username with a manually-configured SSH public key.

Use the **no user-key** command to remove an SSH user and the associated 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

After entering this command, the existing key, if any, associated with the user will be deleted. You must follow this command with the **key-string** command to configure the key to the user. **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
```

13.8 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. The maximum length of a row is 160 characters.
- **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.

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
```

13.9 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 with auto-login.
SSH Password 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
182.20.2.1   Bob Smith      1.5           3DES       Password
```

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) or Password

13.10 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      Fingerprint
-----------   -----------------------------------------------------------
bob           9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
john          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      Fingerprint
-----------   -----------------------------------------------------------
bob           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 *{**console*** | ***telnet*** | ***ssh**}*

Parameters

- **console**—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

Use the **speed** command in Line Configuration mode to set 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 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 only 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

Use the **autobaud** command in Line Configuration mode to configure 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

When this command is enabled, it is activated as follows: connect the console to the device and press the **Enter** key twice. The device detects the baud rate automatically.

Example

The following example enables autobaud.

```
switchxxxxxx(config)# line console
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 telnet session idle time interval before automatic logoff to 20 minutes and 10 seconds.

```
switchxxxxxx(config)# line telnet
switchxxxxxx(config-line)# exec-timeout 20 10
```

14.5 show line

The **show line** EXEC mode command displays line parameters.

Syntax

show line [**console** | ***telnet*** | ***ssh***]

Parameters

- **console**—Displays the console 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
Console 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 aaa authentication enable. 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 aaa authentication enable.

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.
tacacs	Uses the list of all TACACS+ servers for authentication.

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** requests sent by the device to a RADIUS server include the username **$enabx$**., where **x** is the requested privilege level.

All **aaa authentication enable** requests sent by the device to a TACACS+ server include the username that is entered for login authentication.

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 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 15 encrypted
4b529f21c93d4706090285b0c10172eb073ffebc4
```

15.9 service password-recovery

Use the **service password-recovery** Global Configuration mode command to enable the password-recovery mechanism. This mechanism allows an end user, with physical access to the console port of the device, to enter the boot menu and trigger the password recovery process. Use the **no service password-recovery** command to disable the password-recovery mechanism. When the password-recovery mechanism is disabled, accessing the boot menu is still allowed and the user can trigger the password recovery process. The difference is, that in this case, all the configuration files and all the user files are removed. The following log message is generated to the terminal: “All the configuration and user files were removed”.

Syntax

service password-recovery

no service password-recovery

Parameters

N/A

Default Configuration

The service password recovery is enabled by default.

Command Mode

Global Configuration mode

User Guidelines

- If password recovery is enabled, the user can access the boot menu and trigger the password recovery in the boot menu. All configuration files and user files are kept.
- If password recovery is disabled, the user can access the boot menu and trigger the password recovery in the boot menu. The configuration files and user files are removed.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.
- If a device is configured to protect its sensitive data with a user-defined passphrase for (Secure Sensitive Data), then the user cannot trigger the password recovery from the boot menu even if password recovery is enabled.

Example

The following command disables password recovery:

```
switchxxxxxx(config)# no service password recovery
Note that choosing to use Password recovery option in the Boot Menu during
the boot process will remove the configuration files and the user files.
Would you like to continue ? Y/N.
```

15.10 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 MD5 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

Usage Guidelines

See User (Privilege) Levels for an explanation of privilege levels.

- The last level 15 user (regardless of whether it is the default user or any user) cannot be removed.
- The last level 15 user (regardless of whether it is the default user or any user) cannot be demoted

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
```

15.11 show users accounts

The **show users 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 users accounts
                                 Password
Username        Privilege        Expiry date      Lockout
--------        ---------        ----------       --------
Bob             15               Jan 18 2005      0
Robert          15               Jan 19 2005      1
Smith           15                                LOCKOUT
```

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

Field	Description
Username	The user name.
Privilege	The user’s privilege level.
Password Expiry date	The user's password expiration date.
Lockout	If lockout control is enabled, the number of times the user failed to enter the correct password since the last successful login is displayed. If the user account is locked out, LOCKOUT" is displayed.

15.12 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** | **tacacs+**}

no aaa accounting login start-stop

Parameters

- **group radius**—Uses a RADIUS server for accounting.
- **group tacacs+**—Uses a TACACS+ server for accounting.

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/TACACS+ servers in order to select the RADIUS/TACACS+ server.

The following table describes the supported RADIUS accounting attributes values, and in which messages they are sent by the switch.

Name	Start Message	Stop Message	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.

The following table describes the supported TACACS+ accounting arguments and in which messages they are sent by the switch.

Name	Description	Start Message	Stop Message
task_id	A unique accounting session identifier.	Yes	Yes
user	username that is entered for login authentication	Yes	Yes
rem-addr	IP address.of the user	Yes	Yes
elapsed-time	Indicates how long the user was logged in.	No	Yes
reason	Reports why the session was terminated.	No	Yes

Example

```
switchxxxxxx(config)# aaa accounting login start-stop group tacacs
```

15.13 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
```

15.14 show accounting

The **show accounting** EXEC mode command displays information as to which type of accounting is enabled on the switch.

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
```

15.15 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
```

15.16 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
```

15.17 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
```

15.18 passwords lockout

The **passwords lockout** Global Configuration mode command enables user account lockout after a series of authentication failures. Use the **no** form of this command to disable the lockout feature.

Syntax

passwords lockout *number*

no passwords lockout

Parameters

number—Specifies the number of authentication failures before the user account is locked-out. (Range: 1–5)

Default Configuration

Lockout is disabled.

Command Mode

Global Configuration mode

User Guidelines

The setting is relevant to local users' passwords, line passwords and enable passwords.

The account is not locked out for access from the local console.

A user with privilege level 15 can release accounts that are locked out by using the **set username active**, **set enable-password active** and **set line active** Privileged EXEC mode commands.

Disabling lockout unlocks all users.

Re-enabling lockout resets the authentication failures counters.

Changing the authentication failures threshold does not reset the counters.

Example

The following example enables user account lockout after 3 successive authentication failures.

```
switchxxxxxx(config)# passwords lockout 3
```

15.19 aaa login-history file

The **aaa login-history file** Global Configuration mode command enables writing to the login history file. Use the **no** form of this command to disable writing to the login history file.

Syntax

aaa login-history file

no aaa login-history file

Default Configuration

Writing to the login history file is enabled.

Command Mode

Global Configuration mode

User Guidelines

The login history is stored in the device internal buffer.

Example

The following example enables writing to the login history file.

```
switchxxxxxx(config)# aaa login-history file
```

15.20 set username active

The **set username active** Privileged EXEC mode command reactivates a locked out user account.

Syntax

set username *name* **active**

Parameters

name—Specifies the user name: (Length: 1–20 characters)

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example reactivates user ‘Bob’.

```
switchxxxxxx# set username Bob active
```

15.21 set line active

The **set line active** Privileged EXEC mode command reactivates a locked out line.

Syntax

set line *{**console** | **telnet** | **ssh**}* **active**

Parameters

- **console**—Reactivates the console terminal line.
- **telnet**—Reactivates the virtual terminal for remote (Telnet) console access.
- **ssh**—Reactivates the virtual terminal for secured remote (SSH) console access.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example reactivates the virtual terminal for remote (Telnet) console access.

```
switchxxxxxx# set line telnet active
```

15.22 set enable-password active

The **set enable-password active** Privileged EXEC mode command reactivates a locked out local password.

Syntax

set enable-password *level* **active**

Parameters

level—Specifies the privilege level to which the password applies. (Range 1–15)

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Example

The following example reactivates a local password that applies to privilege level 1.

```
switchxxxxxx# set enable-password 1 active
```

15.23 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.

16 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 number of retry retransmissions (Range: 1–15)
- **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). If this parameter is omitted, the globally-configured radius key will be used.
- **key** encrypted-*key-string*—same as key-string, but the key is in encrypted format.
- **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 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 authenticationfor 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 number of retry retransmissions (Range: 1–15)

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
Source IPv6 : ::
```

17 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. The IP address can be an IPv4, IPv6 or IPv6z 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). If this parameter is omitted, the globally-defined key (set in tacacs-server key) will be used.
- **source** *source-ip*—Specifies the source IPv4 or IPv6 address to use for communication. If not specified, the IP address of the outgoing IP interface subnet is used.
- **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 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 or tacacs-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 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 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 tacacs-server source-ipv6

Use the **tacacs-server source-ipv6** Global Configuration mode command to configure the source IPv6 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-ipv6 {*source*}

no tacacs-server source-ipv6 {*source*}

Parameters

source—Specifies the source IPv6 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-ipv6
3ffe:1900:4545:3:200:f8ff:fe21:67cf
```

17.6 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, IP or IPv6 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 logging header enable

Use the **logging header enable** Global Configuration mode command to indicate whether the system should send SYSLOG messages to the server. Use the **no** form of this command to return to the default.

Syntax

logging header enable

no logging header enable

Parameters

N/A

Default Configuration

Sending logging header is Enabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# logging header enable
```

18.14 logging origin-id

Use the **logging origin-id** Global Configuration mode command to configure the origin field of the SYSLOG message packet headers sent to the SYSLOG server. Use the **no** form of this command to return to the default.

Syntax

logging origin-id {***hostname*** | ***IP*** | ***IPv6*** **|** ***string*** *user-defined-id*}

no logging origin-id

Parameters

- **hostname**—The system hostname will be used as the message origin identifier.
- **IP**—IP address of the sending interface that is used as the message origin identifier.
- **IPv6**—IPv6 address of the sending interface that is used as the message origin identifier. If the sending interface is IPv4, the IPv4 address will be used instead.
- **string** *user-defined-id*—Specifies an identifying description chosen by the user. The *user-defined-id* argument is the identifying description string.

Default Configuration

No header is sent apart from the PRI field.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# logging origin-id string “Domain 1, router B”
```

18.15 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.
Logging header sending is enabled
Origin id: hostname
```

```
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
```

18.16 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#
```

18.17 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 port gi1/1/1.

```
switchxxxxxx# show rmon statistics gi1/1/1
Port gi1/1/1
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).

Field	Description
Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
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).

Field	Description
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       gi1/1/1     30        50         50         CLI
2       gi1/1/1     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: gi1/1/1               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:gi1/1/1              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: gi1/1/1             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.

Field	Description
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.
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 which servers used for authentication when 802.1X authentication is enabled. Use the **no** form of this command to restore the default configuration.

Syntax

aaa authentication dot1x default {**radius** | **none** | {**radius none**}}

no aaa authentication dot1x default

Parameters

- **radius** - Uses the list of all RADIUS servers for authentication
- **none** - Uses no authentication

Default Configuration

RADIUS server.

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 no RADIUS server response was received, 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 was received, authentication succeeds.

```
switchxxxxxx(config)# aaa authentication dot1x default radius none
```

20.2 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
```

20.3 dot1x auth-not-req

Use the **dot1x auth-not-req** Interface Configuration (VLAN) mode command to enable unauthorized devices access to the VLAN. Use the **no** form of this command to disable access to the VLAN.

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Parameters

N/A

Default Configuration

Access is enabled.

Command Mode

Interface Configuration (VLAN) mode

User Guidelines

An access port cannot be a member in an unauthenticated VLAN.

The native VLAN of a trunk port cannot be an unauthenticated VLAN.

For a general port, the PVID can be an unauthenticated VLAN (although only tagged packets are accepted in the unauthorized state).

Example

The following example enables unauthorized devices access to VLAN 5.

```
switchxxxxxx(config)# interface vlan 5
switchxxxxxx(config-if)# dot1x auth-not-req
```

20.4 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** command to enable unauthorized users on an interface to access the guest VLAN.

A device can have only one global guest VLAN.

The Guest VLAN must be a static VLAN and it cannot be removed.

Example

The following example defines VLAN 2 as a guest VLAN.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# dot1x guest-vlan
```

20.5 dot1x guest-vlan enable

Use the **dot1x guest-vlan enable** Interface Configuration 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 mode (Ethernet, Port Channel)

User Guidelines

The port cannot belong to 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 enables unauthorized users on `gi1/1/1` to access the guest VLAN.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

20.6 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
```

20.7 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, Port Channel) 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 authorized host can access the network.

Example

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x host-mode multi-host
switchxxxxxx(config-if)# dot1x host-mode single-host
switchxxxxxx(config-if)# dot1x host-mode multi-sessions
```

20.8 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

The guest VLAN must be enabled when MAC authentication is enabled.

Static MAC addresses cannot be authorized. Do not change an authorized MAC address to a static address.

It is not recommended to delete authorized 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 `gi1/1/1`.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x mac-authentication mac-only
```

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, Port Channel) 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 gi1/1/15
switchxxxxxx(config-if)# dot1x max-req 6
```

20.10 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*]

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, Port Channel) 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 gi15 to auto mode.

```
switchxxxxxx(config)# interface gi15
switchxxxxxx(config-if)# dot1x port-control auto
```

20.11 dot1x radius-attributes errors filter-id

Use the **dot1x radius-attributes errors filter-id** 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 cannot 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
```

20.12 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
```

20.13 dot1x radius-attributes vlan

Use the **dot1x radius-attributes vlan** Interface Configuration mode command to enable Radius-based VLAN assignment. Use the **no** form of this command to disable Radius-based VLAN assignment.

Syntax

dot1x radius-attributes vlan [**reject** | *vlan-id*]

no dot1x radius-attributes vlan

Parameters

- **reject**—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN the supplicant is rejected. If the parameter is omitted, this option is applied by default.
- *vlan-id*—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted and the configured VLAN is assigned to the supplicant.

Default Configuration

reject

Command Mode

Interface Configuration (Ethernet, Port Channel) mode

User Guidelines

The configuration of this command is allowed only when the port is Forced Authorized.

RADIUS attributes are supported only in 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, 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.

The command is not supported by the lite multi-sessions mode. See the User Guidelines of the **dot1x host-mode** command for more information.

Example

Example 1. The example enables user-based VLAN assignment. If the RADIUS server authorized the supplicant but did not provide a supplicant VLAN, the supplicant is rejected.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

Example 2. The example enables user-based VLAN assignment. If the Radius server authorized the supplicant but did not provide a supplicant VLAN the supplicant is accepted and VLAN 100 is assigned to the supplicant.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan 100
switchxxxxxx(config-if)# exit
```

20.14 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 gi15:

```
switchxxxxxx# dot1x re-authenticate gi1/1/15
```

20.15 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, Port Channel)

Example

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x reauthentication
```

20.16 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
```

20.17 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: 10–65535 seconds)

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface Configuration (Ethernet, Port Channel) 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.

For 802.1x-Based and MAC-Based authentication methods the quite period is applied after each failed attempt.

Example

The following example sets the time interval that the device remains in the quiet state following a failed authentication exchange to 120 seconds.

```
switchxxxxxx(config)# interface gi1/1/15
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

20.18 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, Port Channel) mode

User Guidelines

The command is only applied to the 802.1x authentication method.

Example

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

20.19 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, Port Channel) 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 gi1/1/15
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

20.20 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, Port Channel) 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.

The command is only applied to the 802.1x authentication method.

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 gi1/1/15
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

20.21 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, Port Channel) 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.

The command is only applied to the 802.1x authentication method.

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 gi15:
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

20.22 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 authorized by the 802.1X mac-authentication access control.

```
switchxxxxxx(config)#interface gi15
switchxxxxxx(config-if)#dot1x traps mac-authentication failure
```

20.23 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 authorized 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 authorized by the 802.1X MAC-authentication access control.

```
switchxxxxxx(config)#interface gi15
switchxxxxxx(config-if)#dot1x traps mac-authentication success
```

20.24 dot1x violation-mode

Use the **dot1x violation-mode** Interface Configuration mode command to configure the action to be taken, when an unauthorized host on authorized port in single-host mode, 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, Port Channel) 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 gi1/1/1
switchxxxxxx(config-if)# dot1x violation-mode protect
```

20.25 show dot1x

Use the **show dot1x** Privileged EXEC mode command to display the 802.1X interfaces or specified interface status.

Syntax

show dot1x [**interface** *interface-id* **| detailed**]

Parameters

- *interface-id*—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

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 gi1/1/3
802.1X is enabled.
Port       Admin        Oper           Reauth     Reauth   Username
           Mode         Mode           Control    Period
----       ----------   ------------   -------    ------   --------
gi1/1/3    Auto         Unauthorized   Enable     3600     Clark
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
----       ----------         ------------   -------    ------   --------
gi1/1/1    Auto               Authorized     Enable     3600     Bob
gi1/1/2    Auto               Authorized     Enable     3600     John
gi1/1/3    Auto               Unauthorized   Enable     3600     Clark
gi1/1/4    Force-authorized   Authorized     Disable    3600     n/a
gi1/1/5    Force-authorized   Unauthorized   Disable    3600     n/a
* 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.

Field	Description
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 authorized 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.

```
Time range name: work_hours
Time range name: work_hours
Time range name: work_hours
```

20.26 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* **|** ***detailed***]

Parameters

- *interface-id*—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

Example

20.27 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 `gi1/1/1`.

```
switchxxxxxx# show dot1x statistics interface gi1/1/1
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.

20.28 show dot1x users

Use the **show dot1x users** Privileged EXEC mode command to display active 802.1X authorized 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
--------- -----------------------------  -----------      ----
gi1/1/1 Bob        1d 09:07:38   Remote    0008.3b79.8787    3
```

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, OOB, IP interface or tunnel) mode

Examples

Example 1 - For Gigabit Ethernet ports:

```
switchxxxxxx(config)# interface gi1/1/1
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 gi1/1/1-20
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 `gi1/1/5` operations.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# shutdown
switchxxxxxx(config-if)#
```

Example 2 - The following example restarts the disabled Ethernet port.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# no shutdown
switchxxxxxx(config-if)
```

21.4 operation time

Use the **operation time** Interface Configuration (Ethernet) mode command to control the time that the port is up. Use the **no** form of this command to cancel the time range for the port operation time.

Syntax

operation time *time-range-name*

no operation time

Parameters

- **time-range-name**—Specifies a time range the port operates (in up state). When the Time Range is not in effect, the port is shutdown. (Range: 1–32 characters)

Default Configuration

There is no time range configured on the port 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 operation time command influences the port if the port status is up. This command defines the time frame during which the port stays up and at which time the port will be shutdown. While the port is in shutdown because of other reasons, this command has no effect.

The following example activates an operation time range (named "morning") on port gi1/1/15.

```
Console(config)# interface gi1/1/15
Console(config-if)# operation time morning
```

21.5 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 gi1/1/5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# description SW#3
```

21.6 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* | *10000}*

no speed

Parameters

- **10**—Forces10 Mbps operation
- **100**—Forces 100 Mbps operation
- **1000**—Forces 1000 Mbps operation
- **10000**—Forces 10000 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 gi1/1/5 to 100 Mbps operation.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# speed 100
```

21.7 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 gi1/1/5 to operate in full duplex mode.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# duplex full
```

21.8 negotiation

Use the **negotiation** Interface Configuration (Ethernet, Port-channel) mode command to enable auto-negotiation operation for the speed and duplex parameters and master-slave mode of a given interface. Use the **no** form of this command to disable auto-negotiation.

Syntax

negotiation [*capability* [*capability2*... *capability5*]] [preferred {master | slave}]

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
- Preferred - Specifies the master-slave preference:
  - Master - Advertise master preference
  - Slave - Advertise slave preference

Default Configuration

If capability is unspecified, defaults to list of all the capabilities of the port and preferred master mode.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

Example

The following example enables auto-negotiation on gi1/1/5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# negotiation
```

21.9 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 gi1/1/1

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# flowcontrol on
```

21.10 flowcontrol

Use the **flowcontrol** Global Configuration mode command to configure the Flow Control global mode.

Syntax

flowcontrol {***receive-only*** | ***send-receive***}

Parameters

- **receive-only**—The interfaces with enabled Flow Control will receive pause frames, but will not send Flow Control pause frames.
- **send-receive**—The interfaces with enabled Flow Control will receive and send pause frames.

Default Configuration

receive-only.

Command Mode

Global Configuration

User Guidelines

Flowcontrol must also be enabled on the specific interfaces required. This command only determines the global mode and does not enable/disable Flow Control on any interface.

Example

The following example enables Flow Control in the mode of only receiving pause frames and not sending them.

```
switchxxxxxx(config)# flowcontrol receive-only
```

21.11 show flowcontrol

Use the **show flowcontrol** Exec mode command to display the Flow Control global mode..

Syntax

show flowcontrol

Parameters

N/A

Default Configuration

N/A

Command Mode

Exec mode

Example

The following example displays the Flow Control global mode.

```
switchxxxxxx# show flowcontrol
```

21.12 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 gi1/1/5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# mdix auto
```

21.13 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

Example

The following example enables back pressure on port gi1/1/5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# back-pressure
```

21.14 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
```

21.15 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 `gi1/1/5`.

```
switchxxxxxx# clear counters gi1/1/5.
```

21.16 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 `gi1/1/1`.

```
switchxxxxxx# set interface active gi1/1/1
```

21.17 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
```

21.18 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
```

21.19 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* **|** ***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.

Default Configuration

Display all interfaces. If detailed is not used, only present ports are displayed.

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
------ --------- ------  -----  -------- -------  -----  --------  ----
gi1/1/1   1G-Copper Full    10000  Disabled Off      Up     Disabled  Off
gi1/1/2   1G-Copper Full    1000   Disabled Off      Up     Disabled  Off
                                 Flow      Admin
PO      Type   Speed  Neg        Control   State
------  ------ -----  --------   -------   -----
Po1                   Disabled   Off       Up
```

21.20 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. If detailed is not used, only present ports are displayed.

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
------ --------- ------ ----- -------- ----  ------ -------- --
gi1/1/1   1G-Copper Full   1000  Disabled Off   Up     Disabled Off
gi1/1/2   1G-Copper --     --     --       --    Down   --       --
                                       Flow     Link
PO     Type      Duplex Speed  Neg     control  State
```

```
-----  -------   ------ -----  ------- ----     ------
Po1    1G        Full   10000  Disabled Off     Up
```

21.21 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* **|** ***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.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Examples

The following examples display auto-negotiation information.

```
switchxxxxxx# show interfaces advertise
Port      Type        Neg                 Operational Link
----      ---------   ------              Advertisement
gi1/1/1   1G-Copper   Enable              -----------------------------
gi1/1/2   1G-Copper   Enable              -
                                          1000f, 100f, 10f, 10h
                                          1000f
switchxxxxxx# show interfaces advertise gi1/1/1
Port:gi1/1/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
```

```
                                         10h   10f   100h   100   1000f
                                         ---   ---   ----   f     -----
Admin Local link                         yes   yes   yes    ---   yes
Advertisement                            yes   yes   yes    -     yes
Oper Local link Advertisement            no    no    yes    yes   yes
Remote Local link                        -     -     -      yes   yes
Advertisement                                               yes
Priority Resolution                                         -
switchxxxxxx# show interfaces advertise gi1/1/1
Port: gi1/1/1
Type: 1G-Copper
Link state: Up
Auto negotiation: disabled.
```

21.22 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* **|** ***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.

Default Configuration

Display description for all interfaces.If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following example displays the description of all configured interfaces.

```
switchxxxxxx# show interfaces description
```

```
Port        Descriptions
gi1/1/1     ---------------------------------------------
gi1/1/2     Port that should be used for management only
gi1/1/3
gi1/1/4
PO          Description
----        -----------
Po1         Output
```

21.23 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* **|** ***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.

Default Configuration

Display counters for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

The following example displays traffic seen by all the physical interfaces.

```
switchxxxxxx# show interfaces counters gi1/1/1
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
gi1/1/1          0            0            0            0
Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
gi1/1/1          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.

21.24 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 ports 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
```

21.25 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
```

21.26 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
------------        ------------------
gi1/1/50            stp-bpdu-guard
```

21.27 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 gi1/1/1
switchxxxxxx(config-if)# storm-control broadcast enable
```

21.28 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

kbps—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 gi1/1/1
switchxxxxxx(config-if)# storm-control broadcast level kbps 12345
```

21.29 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

no storm-control include-multicast

Default Configuration

Disabled

Command Mode

Interface Configuration mode (Ethernet)

Example

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# storm-control include-multicast
```

21.30 show storm-control

Use the **show storm-control** EXEC mode command to display the configuration of storm control for all ports or for a specific one.

Syntax

show storm-control *[interface-id* **|** ***detailed***]

Parameters

- **interface-id**—Specifies an Ethernet port.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

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).

If the suppression level in percentage is translated to a rate that is lower than the minimum rate, the minimum rate is set.

Example

```
switchxxxxxx# show storm-control
Port   State    Rate [Kbits/Sec]  Included
------ -------- ---------------   ------------------------
gi1/1/1    Enabled  12345            Broadcast, Multicast,
                                  Unknown unicast
gi1/1/2    Disabled 100000           Broadcast
```

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

This command does not work on fiber ports (if they exist on the device). The port to be tested should be shut down during the test, unless it is a combination port with fiber port active. In this case, it does not need to be shut down, because the test does not work on fiber ports.

The maximum length of cable for the TDR test is 120 meters.

Example

Example 1 - Test the copper cables attached to port 1 (a copper port).

```
switchxxxxxx# test cable-diagnostics tdr interface gi1/1/1
Cable is open at 64 meters
```

Example 2 - Test the copper cables attached to port 2 (a combo port with fiber active).

```
switchxxxxxx# test cable-diagnostics tdr interface gi1/1/2
Fiber ports are not supported
```

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* **|** ***detailed***]

Parameters

- **interface-id**—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present 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]        ------------------
                    ------------

gi1/1/1   OK

gi1/1/2   Short     50              13:32:00 23 July 2010

gi1/1/3   Test has not been performed

gi1/1/4   Open      64              13:32:00 23 July 2010
```

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* **|** ***detailed***]

Parameters

- **interface-id**—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present 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]
----           -----------------
gi1/1/1        < 50
gi1/1/2        Copper not active
gi1/1/3        110-140
```

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 iber-ports optical-transceiver *[**interface** interface-id* **|** ***detailed***]

Parameters

- **interface-id**—Specify an Ethernet port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

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
----------- ------ ------- -------  ------ -----   ---
   gi1/1/1      W       OK      OK     OK     OK      OK
   gi1/1/2      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
   Port      Temp  Voltage Current Output  Input   LOS
             [C]   [Volt]  [mA]    Power   Power
                                   [mWatt] [mWatt]
----------- ------ ------- ------- ------- ------- ---
  gi1/1/1     Copper
  gi1/1/6     Copper
  gi1/1/7      28    3.32    7.26    3.53    3.68   No
  gi1/1/8      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

??

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

??

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 gi1/1/1
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 gi1/1/1
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 gi1/1/1
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.

Techaya recommends a default of 50m for any cable type.

However, Techaya 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 gi1/1/1
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# 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* **|** ***detailed***]

Parameters

- **interface-id**—Specifies an Ethernet port
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

Command Mode

Privileged EXEC mode

User Guidelines

The power savings displayed is only relevant to the power saved by short reach and energy detect.

The EEE power saving is dynamic by nature since it is based on port utilization and is therefore not taken into consideration.

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 exceeds threshold
6	LD	Port Link is Down – NA

Example

```
switchxxxxxx# show green-ethernet
Energy-Detect mode: Enabled
Short-Reach mode: Disabled
Power Savings: 24% (1.08W 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
----  ----- ---- -------  ----- ----- ---- -------  ------
gi1/1/1   on    on             off  off   off
gi1/1/2   on    off  LU        on   off   off           < 50
gi1/1/3   on    off  LU        off  off   off
```

24 Port Channel Commands

24.1 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 `gi1/1/1` to join port-channel 1 without an LACP operation.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# channel-group 1 mode on
```

24.2 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**}*

no port-channel load-balance

Parameters

- **src-dst-mac**—Port channel load balancing is based on the source and destination MAC addresses.
- **src-dst-mac-ip**—Port channel load balancing is based on the source and destination of MAC and IP addresses.

- **src-dst-ip**—Port channel load balancing is based on the source and destination IP addresses.

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
```

24.3 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

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: gi1/1/1,Inactive: gi1/1/2-3
Po2      Active: gi1/1/5 Inactive: gi1/1/4
```

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
gi1/1/1-2
```

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 gi1/1/9 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 gi1/1/9
```

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
gi1/1/9
```

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 `gi1/1/9` 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 gi1/1/9
```

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 gi1/1/9 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 gi1/1/9
```

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 gi1/1/1-2
```

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 `gi1/1/9` 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 gi1/1/9
```

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 gi1/1/9 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 gi1/1/9
```

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 gi1/1/1:

```
switchxxxxxx(config)# interface gi1/1/1
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 gi1/1/8 to be forwarded.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forward-all add gi1/1/8
```

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 gi1/1/1 within VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge multicast forbidden forward-all add
ethernet gi1/1/1
```

25.17 bridge unicast unknown

Use the **bridge unicast unknown** Interface Configuration mode command to enable egress filtering of Unicast packets where the destination MAC address is unknown to the device. Use the **no** form of this command to restore the default configuration.

Syntax

bridge unicast unknown {***filtering*** | ***forwarding***}

no bridge unicast unknown

Parameters

- **filtering**—Filter unregistered Unicast packets.
- **forwarding**—Forward unregistered Unicast packets.

Default Configuration

Forwarding.

Command Mode

Interface Configuration mode

Example

The following example drops Unicast packets on VLAN 2 when the destination is unknown.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# bridge unicast unknown filtering
```

25.18 show bridge unicast unknown

Use the **show bridge unicast unknown** command to display the unknown Unicast filtering configuration.

Syntax

show bridge unicast unknown [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

Command Mode

EXEC

Example

```
Console # show bridge unicast unknown

Port          Unregistered
------        -------------
1/1           Forward
1/2           Filter
1/3           Filter
```

25.19 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. 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
interface gi1/1/1
switchxxxxxx(conf)mac address-table static 00:3f:bd:45:5a:b2 vlan 1
interface gi1/1/1 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
interface gi1/1/1 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
interface gi1/1/1 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
interface  gi1/1/1 secure
```

25.20 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
```

25.21 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:10-630)

Default Configuration

10-630

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# mac address-table aging-time 600
```

25.22 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 bridge unicast unknown 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 gi1/1/1 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 gi1/1/7
switchxxxxxx(config-if)port security mode lock
switchxxxxxx(config-if)port security forward trap 100
switchxxxxxx(config-if)exit
```

25.23 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

port security mode {**max-addresses | lock** | **secure permanent |secure delete-on-reset**}

no port security mode

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 bridge unicast unknown command.
- **lock**—Secure mode without MAC learning. The static and secure MAC addresses may be added on the port manually by the bridge unicast unknown command.
- **secure permanent**—Secure mode with limited learning permanent secure MAC addresses with the **permanent** time-of-live. The static and secure MAC addresses may be added on the port manually by the **mac address-table static** command.

- **secure delete-on-reset**—Secure mode with limited learning secure MAC addresses with the **delete-on-reset** time-of-live. 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 bridge unicast unknown 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 gi1/1/7.

```
switchxxxxxx(config)interface gi1/1/7
switchxxxxxx(config-if)port security mode lock
switchxxxxxx(config-if)port security
switchxxxxxx(config-if)exit
```

25.24 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
```

25.25 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 gi1/1/1.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# port security routed secure-address
00:66:66:66:66:66
```

25.26 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**—Displays 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     gi1/1/1       static
   1       00:a1:b0:69:63:f3     gi1/1/4       dynamic
   2       00:a1:b0:69:63:f3     gi1/1/5       dynamic
```

Example 2 - Displays address table entries containing the specified MAC address.

```
switchxxxxxx# show mac address-table address 00:3f:bd:45:5a:b1
Aging time is 300 sec
VLAN        MAC Address         Port       Type
-------- -------------------- ---------- ----------
1         00:3f:bd:45:5a:b1    static      gi1/1/9
```

25.27 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
This may take some time.
Capacity : 16384
Free     : 16379
Used     : 5
Secure   : 0
Dynamic  : 2
Static   : 2
Internal : 1
console#
```

25.28 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
```

25.29 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      gi1/1/9
Multicast address table for VLANs in IPv4-GROUP bridging mode:
Vlan    MAC Address         Type             Ports
---- -----------------    --------------     -----
1      224.0.0.251         Dynamic           gi1/1/2
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     gi1/1/1
Forbidden ports for Multicast addresses:
Vlan  Group Address  Source Address   Ports
---- --------------- --------------- -------
8    239.2.2.2       *               gi1/1/9
8    239.2.2.2       1.1.1.11        gi1/1/9
Multicast address table for VLANs in IPv6-GROUP bridging mode:
VLAN  IP/MAC Address   Type      Ports
---- ----------------- --------- ---------------------
8    ff02::4:4:4       Static    gi1/1/1-2, gi1/1/7, Po1
Forbidden ports for Multicast addresses:
VLAN  IP/MAC Address   Ports
---- ----------------- -----------
```

```
8    ff02::4:4:4       gi1/1/9
Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:
Vlan  Group Address  Source address  Type     Ports
---- --------------- --------------- -------- ------------------
8    ff02::4:4:4     *               Static   gi1/1/1-2,gi1/1/7,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     *                  gi1/1/9
8    ff02::4:4:4     fe80::200:7ff:f    gi1/1/9
                     e00:200
```

25.30 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     gi1/1/1, gi1/1/2

Forbidden ports for multicast addresses:

Vlan       MAC Address        Ports
----       --------------     --------

IPv4-GROUP Table

Vlan       IP Address         Ports
----       ----------         --------
1          231.2.2.3          gi1/1/1, gi1/1/2
19         231.2.2.8          gi1/1/-8
19         231.2.2.8          gi1/1/9-21

Forbidden ports for multicast addresses:

Vlan       IP Address         Ports
----       ----------         --------
1          231.2.2.3          gi1/1/8
19         231.2.2.8          gi1/1/3

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        FF12::8            gi1/1/1-8

Forbidden ports for multicast addresses:

Vlan       IP Address         Ports
----       ----------------   ---------
11         FF12::3            gi1/1/8
191        FF12::8            gi1/1/8

IPv6-SRC-GROUP Table:
```

```
Vlan      Group Address     Source             Ports
----      ---------------   address            ------
192       FF12::8           ---------------    gi1/1/1-8
                            FE80::201:C9A9:FE40
                            :8988
Forbidden ports for multicast addresses:
Vlan      Group Address     Source             Ports
----      ---------------   address            ------
192       FF12::3           ---------------    gi1/1/8
                            FE80::201:C9A9:FE40
                            :8988
```

25.31 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
Forward-All
Port        Static        Status
-----       ---------     ------
gi1/1/1     Forbidden     Filter
gi1/1/2     Forward       Forward(s)
gi1/1/3     -             Forward(d)
```

25.32 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
-------    -------------
gi1/1/1    Forward
gi1/1/2    Filter
gi1/1/3    Filter
```

25.33 show ports security

Use the **show ports security** Privileged EXEC mode command to display the port-lock status.

Syntax

show ports security *[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.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

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
------- --------  ---------   ------    ---      -------  --------
gi1/1/1     Enabled   Max-        Discard   3        Enabled 100
                  Addresses
gi1/1/2     Disabled  Max-        -         28       -        -
                  Addresses
gi1/1/3     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.

25.34 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* **|** ***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.

Default Configuration

Display for all interfaces. If detailed is not used, only present ports are displayed.

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
...
```

25.35 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
```

25.36 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 `gi1/1/2` to destination port `gi1/1/1`.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# port monitor gi1/1/2
```

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
Global Port Monitor Sessions is enabled

Source port     Destination Port   Type      Status
-----------   ----------------    --------  --------
gi1/1/8             gi1/1/1                 RX,TX     Active
gi1/1/2             gi1/1/1                 RX,TX     Active
gi1/1/18         gi1/1/1             Rx        Active
VLAN 9         gi1/1/1            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
----- -----------     --------- ---------   ---------- -----   ------------
gi1/1/1   1/2048     60 sec    128         1                  1
gi1/1/2   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            Datagrams sent
               sampled            to collector
 ----------    -----------        --------------
 gi1/1/1       30                 50
 gi1/1/2       30                 50
 gi1/1/3       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 gi1/1/1
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 gi1/1/1
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 optional-tlv

Use the **lldp optional-tlv** Interface Configuration (Ethernet) mode command to specify which optional TLVs are transmitted. Use the **no** form of this command to restore the default configuration.

For 802.1, see the lldp optional-tlv 802.1 command.

Syntax

lldp optional-tlv *tlv* [*tlv2 … tlv5* | ***none***]

Parameters

- **tlv**—Specifies the TLVs to be included. Available optional TLVs are: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size.
- **none**—Clear all optional TLVs from the interface.

If the 802.1 protocol is selected, see the command below.

Default Configuration

No optional TLV is transmitted.

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example specifies that the port description TLV is transmitted on gi1/1/2.

```
Console(config)# interface gi1/1/2
Console(config-if)# lldp optional-tlv port-desc
```

28.9 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*—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 gi1/1/2.

```
Console(config)# interface gi1/1/2
Console(config-if)# lldp management-address automatic
```

28.10 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 gi1/1/5.

```
Console(config)# interface gi1/1/5
Console(config-if)# lldp notifications enable
```

28.11 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
```

28.12 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, 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 gi1/1/3.

```
Console(config)# interface gi1/1/3
Console(config-if)# lldp med enable location
```

28.14 lldp med

Use the **lldp med** Interface Configuration (Ethernet) mode command to enable or disable LLDP Media Endpoint Discovery (MED) on a port. Use the **no** form of this command to return to the default state.

Syntax

lldp med {*enable* [*tlv … tlv4*] | ***disable***}

no lldp med

Parameters

- **enable** - Enable LLDP MED
- **tlv**—Specifies the TLV that should be included. Available TLVs are: network-policy, location, inventory. The capabilities TLV is always included if LLDP-MED is enabled.
- **disable** - disable LLDP MED on the port

Default Configuration

Disabled

Command Mode

Interface Configuration (Ethernet) mode

Example

The following example enables LLDP MED with the **location** TLV on gi1/1/3.

```
Console(config)# interface gi1/1/3
Console(config-if)# lldp med enable location
```

28.15 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 `gi1/1/2`.

```
Console(config)# interface gi1/1/2
Console(config-if)# lldp med notifications topology-change enable
```

28.16 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
```

28.17 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 gi1/1/1
Console(config-if)# lldp med network-policy add 1
```

28.18 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 gi1/1/1
Console(config-if)# lldp med network-policy add 1
```

28.19 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 gi1/1/1
```

28.20 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 `gi1/1/2` as a civic address.

```
console(config)# interface gi1/1/2
console(config-if)# lldp med location civic-address 616263646566
```

28.21 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* **|** ***detailed***]

Parameters

- **interface-id**—Specifies the port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Display for all ports. If detailed is not used, only present ports are displayed.

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

Port      State  Optional TLVs      Address       Notifications
--------  -----  --------------     -----------   ------------
gi1/1/1       RX,TX  PD, SN, SD, SC      172.16.1.1    Disabled
gi1/1/2       TX     PD, SN              172.16.1.1    Disabled
gi1/1/3       RX,TX  PD, SN, SD, SC      None          Disabled
gi1/1/5       RX,TX  D,  SN, SD, SC      automatic     Disabled
gi1/1/6       RX,TX  PD, SN, SD, SC      auto vlan 1   Disabled
gi1/1/7       RX,TX  PD, SN, SD, SC      auto g1       Disabled
gi1/1/8   RX,TX  PD, SN, SD, SC      auto ch1      Disabled
```

Example 2 - Display LLDP configuration for port 1.

```
Switch# show lldp configuration gi1/1/1
 State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
Port State      Optional TLVs     Address      Notifications
---- ---------- --------------    -----------  -----------
gi1/1/1  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.
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.

28.22 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* **|** ***detailed***]

Parameters

- **interface-id**—Specifies the port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

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
------ -------------- -------------- ---------- -------------   --------
gi1/1/1   Yes             Yes            Yes         Enabled        Yes
gi1/1/2   Yes             Yes            No          Enabled        No
gi1/1/3   No              No             No          Enabled        No
```

Example 2 - The following example displays the LLDP MED configuration for gi1/1/1.

```
console# show lldp med configuration gi1/1/1

Port    Capabilities   Network Policy   Location  Notifications Inventory
------- -------------- ---------------- --------- ----------    --------
gi1/1/1    Yes             Yes             Yes       Enabled        Yes
Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

28.23 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 gi1/1/1
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
```

28.24 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 gi1/1/1 and 2.

```
Switch# show lldp local gi1/1/1
Device ID: 0060.704C.73FF
Port ID: gi1/1/1
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 gi1/1/2
LLDP is disabled.
```

28.25 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
System capability legend:
B - Bridge; R - Router; W - Wlan Access Point; T - telephone;
D - DOCSIS Cable Device; H - Host; r - Repeater;
TP - Two Ports MAC Relay; S - S-VLAN; C - C-VLAN; O - Other
Port  Device ID         Port ID  System Name Capabilities TTL
----- ---------------   -------- ----------  -----------  ----
gi1/1/1 00:00:00:11:11:11   gi1/1/1      ts-7800-2   B            90
gi1/1/1 00:00:00:11:11:11   gi1/1/1      ts-7800-2   B            90
gi1/1/2 00:00:26:08:13:24   gi1/1/3      ts-7900-1   B, R         90
gi1/1/3 00:00:26:08:13:24   gi1/1/2      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 gi1/1/1
Device ID: 00:00:00:11:11:11
Port ID: gi1/1/1
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.
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.

Field	Description
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).
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.

28.26 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* **|** ***detailed***]

Parameters

- **interface-id**—Specifies the port ID.
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

If no port ID is entered, the command displays information for all ports. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

```
switchxxxxxx# 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
----- ---- ----- --------- --------- ---------   ---------    ------------
gi1/1/1   730   850    0       0         0             0          0
gi1/1/2   0      0     0       0         0             0          0
gi1/1/3   730    0     0       0         0             0          0
gi1/1/4   0      0     0       0         0             0          0
gi1/1/5   0      0     0       0         0             0          0
gi1/1/6   8      7     0       0         0             0          1
gi1/1/7   0      0     0       0         0             0          0
gi1/1/8   0      0     0       0         0             0          0
gi1/1/9   730    0     0       0         0             0          0
gi1/1/10  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 mst
```

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 gi1/1/5

```
switchxxxxxx(config)# interface gi1/1/5
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
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 gi1/1/15 to 35000.

```
switchxxxxxx(config)# interface gi1/1/15
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 gi1/1/15 to 96

```
switchxxxxxx(config)# interface gi1/1/15
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 gi1/1/15.

```
switchxxxxxx(config)# interface gi1/1/15
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 gi1/1/15.

```
switchxxxxxx(config)# interface gi1/1/15
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: 1–200,000,000.

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 the default cost as 100.
- If the long method is selected, the switch calculates the default cost as 20000.

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 `gi1/1/3`**.**

```
switchxxxxxx(config)# interface gi1/1/3
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 `gi1/1/1` from being the root port of the device.

```
switchxxxxxx(config)# interface gi1/1/1
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 `gi1/1/5` when it receives a BPDU.

```
switchxxxxxx(config)# interface gi1/1/5
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:1–15)
- **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 gi1/1/1 to 144.

```
switchxxxxxx(config)# interface gi1/1/1
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
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 port `gi1/1/9` to 4.

```
switchxxxxxx(config)# interface gi1/1/9
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                gi1/1/1

           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
------     ------  ------      -----  ---    ----  -------  ----------
gi1/1/1    Enabled 128.1       20000  FRW    Root  No       P2p (RSTP)
gi1/1/2    Enabled 128.2       20000  FRW    Desg  No       Shared (STP)
gi1/1/3    Disabled 128.3      20000  -      -     -        -
gi1/1/4    Enabled 128.4       20000  BLK    Altn  No       Shared (STP)
gi1/1/5    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    PortFastType
--------   -----------------   -----  ---    ----    ------------------
gi1/1/1    Enabled 128.1       20000  FRW    Desg    -       P2p (RSTP)
gi1/1/2    Enabled 128.2       20000  FRW    Desg    No      Shared (STP)
gi1/1/3    Disabled128.3       20000  -      -       No      -
gi1/1/4    Enabled 128.4       20000  FRW    Desg    -       Shared (STP)
gi1/1/5    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    PortFastType
---------  ---------------     -----  ---    ----    ------------------
gi1/1/1    Enabled 128.1       20000  -      -       -       -
gi1/1/2    Enabled 128.2       20000  -      -       -       -
gi1/1/3    Disabled128.3       20000  -      -       -       -
gi1/1/4    Enabled 128.4       20000  -      -       -       -
gi1/1/5    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           gi1/1/1

           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
---------  -------- ------      -----   ---     ----     -------- ---------
gi1/1/1    Enabled  128.1       20000   FRW     Root     -        P2p (RSTP)
gi1/1/2    Enabled  128.2       20000   FRW     Desg     No       Shared (STP)
gi1/1/4    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            gi1/1/1

           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
---------  -------  ------      -----   ---     ----     -------- ---------
gi1/1/4    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            gi1/1/1

           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 (gi1/1/1) 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 (gi1/1/2) 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 (gi1/1/3) 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 (gi1/1/4) 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 (gi1/1/5) 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 gi1/1/1

Port 1 (gi1/1/1) 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   gi1/1/1

                   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
----       -------  --------    -----   ---     ----    --------------------
gi1/1/1    Enabled  128.1       20000   FRW     Root    No       P2p Bound
gi1/1/2    Enabled  128.2       20000   FRW     Desg    No       (RSTP)
gi1/1/3    Enabled  128.3       20000   FRW     Desg    No       Shared Bound
gi1/1/4    Enabled  128.4       20000   FRW     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    gi1/1/4
                   Rem hops    19


Bridge ID          Priority    32768
                   Address     00:02:4b:29:7a:00

Interfaces

Name       State    Prio.Nbr    Cost    Sts    Role    PortFast Type
----       -------  --------    -----   ---    ----    -------- ------------
gi1/1/1    Enabled  128.1       20000   FRW    Boun    No       P2p Bound
gi1/1/2    Enabled  128.2       20000   FRW    Boun    No       (RSTP)
gi1/1/3    Enabled  128.3       20000   BLK    Altn    No       Shared Bound
gi1/1/4    Enabled  128.4       20000   FRW    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    gi1/1/1

                   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 (gi1/1/1) 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 (gi1/1/2) 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 (gi1/1/3) 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 (gi1/1/4) 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    gi1/1/4

                   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 (gi1/1/1) 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 (gi1/1/2) 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 (gi1/1/3) 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 (gi1/1/4) 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    gi1/1/1
                   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    gi1/1/1
                   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* **|** ***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.

Default Configuration

Show information for all interfaces. If detailed is not used, only present ports are displayed.

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
---------       ----------      ---------
gi1/1/1         Filtering       Filtering
gi1/1/2         Filtering       Filtering
gi1/1/3         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
---------       ----------      ---------
gi1/1/1         Global          Flooding
gi1/1/2         Global          STP
gi1/1/3         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     gi1/1/1-2     Default       Required
10     Marketing   gi1/1/3-14    Static        Required
11     VLAN0011    gi1/1/5-16    Static        Required
20     VLAN0020    gi1/1/7-18    Static        Required
21     VLAN0021                  Static        Required
30     VLAN0030                  Static        Required
31     VLAN0031                  Static        Required
91     VLAN0091    gi1/1/2       Dynamic       Not Required
3978   Guest       gi1/1/7       Static        Guest
       VLAN
```

Example 2 - The following example displays information for the default VLAN (VLAN 1):

```
switchxxxxxx# show vlan tag 1


VLAN   Name        Ports         Type         Authorization
----   ---------   --------      -------      -------------
1      default     gi1/1/1-2     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   gi1/1/3-14    static       Required
```

30.4 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

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
```

30.5 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.

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)#
```

30.6 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
```

30.7 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 gi1/1/1
switchxxxxxx(config-if)# switchport protected-port
```

30.8 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* **|** ***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.

Default Configuration

Show all protected interfaces. If detailed is not used, only present ports are displayed.

Command Mode

EXEC mode

Example

```
switchxxxxxx# show interfaces protected-ports
Interface     State      Community
--------- -------------  ---------
  gi1/1/1      Protected       1
  gi1/1/2      Protected       Isolated
  gi1/1/3      Unprotected     20
  gi1/1/4      Unprotected     Isolated
```

Note: The Community column for unprotected ports is relevant only when the port state is changed to Protected.

30.9 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 gi1/1/1
switchxxxxxx(config-if)# switchport community 1
```

30.10 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
```

30.11 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 gi1/1/1 as an access port (untagged layer 2) VLAN port.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

30.12 switchport access vlan

An interface in access mode can belong to only one VLAN. The **switchport access vlan** Interface Configuration command reassigns an interface to a different VLAN than it currently belongs to.

Use the **no** form of this command to restore the default configuration.

Syntax

switchport access vlan *vlan-id*

no switchport access vlan

Parameters

vlan *vlan-id*—Specifies the VLAN ID to which the port is configured.

Default Configuration

The interface belongs to the default VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

The command automatically removes the port from its previous VLAN and adds it to the new VLAN.

If the interface is a forbidden member of the added VLAN, the interface does not become a member of this VLAN. The system displays an error message about this ("An interface cannot become a a member of a forbidden VLAN. This message will only be displayed once.").

Example

The following example sets gi1 as an access port and assigns it to VLAN 2 (and removes it from its previous VLAN).

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

30.13 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 the default VLAN.

Command Mode

Interface Configuration (Ethernet, port-channel) mode

User Guidelines

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. The system displays an error message about this issue ("An interface cannot become a a member of a forbidden VLAN. This message will only be displayed once."), and the command continues to execute in case there are more VLANs in the vlan-list.

Example

To add VLANs 2,3 and 100 to trunk ports 1 to 13:

```
switchxxxxxx(config)# interface range gi1/1/1-13
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
switchxxxxxx(config-if)#
```

30.14 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*

no switchport trunk native vlan

Parameters

- **vlan-id**—Specifies the native VLAN ID.

Default Configuration

The default VLAN is the native VLAN.

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.

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. There will be an error message in this case ("An interface cannot become a a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute if there are more VLANs in the vlan-list.

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 gi1/1/1
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 gi1/1/1
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 as tagged on ingress and tagged on egress:

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2
switchxxxxxx(config-if)#
```

30.15 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.

If the interface is a forbidden member of an added VLAN, the interface does not become a member of this specific VLAN. There will be an error message in this case ("An interface cannot become a a member of a forbidden VLAN. This message will only be displayed once.") and the command continues to execute if there are more VLANs in the vlan-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 gi1/1/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

30.16 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 gi1/1/2
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 gi1/1/14
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 gi1/1/14
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 gi1/1/21
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 gi1/1/14
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 gi1/1/23
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general allowed vlan add 2 tagged
switchxxxxxx(config-if)#
```

30.17 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 gi1/1/1.

```
switchxxxxxx(config)# interface gi1/1/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

30.18 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 `gi1/1/3` to be in general mode and to discard untagged frames at ingress.

```
switchxxxxxx(config)# interface gi1/1/3
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type
tagged-only
```

30.19 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 gi1/1/5 as a member of customer VLAN 5.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

30.20 switchport protected

Use the **switchport protected** Interface Configuration (Ethernet, Port-channel) mode command to override the Filtering Database (FDB) decision, and send all Unicast, Multicast and Broadcast traffic to an uplink port. Use the **no** form of this command to disable overriding the FDB decision.

Syntax

switchport protected *{interface-id}*

no switchport protected

Parameters

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

Default Configuration

Switchport protected mode is disabled.

Command Mode

Interface Configuration (Ethernet, Port-channel) mode

User Guidelines

This command overrides the FDB decision, and forwards packets to the uplink. Note that the packet is still subject to all filtering decisions.

A protected port cannot be a member of a VLAN with an IP interface.

Example

This example configures gi1/1/2 as a protected port, so that all traffic is sent to its uplink (gi1/1/3).

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# switchport protected gi1/1/3
```

30.21 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-value*] **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-value**—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 value 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
```

30.22 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
```

30.23 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

Encapsulation          Protocol              Group ID
-------------          --------------        --------
Ethernet               0x800 (IP)            1
Ethernet               0x806 (ARP)           1
Ethernet               0x86dd (IPv6)         2
Ethernet               0x8898                3
```

30.24 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.

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 gi1/1/11
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
```

30.25 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 gi1/1/11
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
```

30.26 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
```

30.27 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
```

30.28 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
```

30.29 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
```

30.30 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 gi1/1/7.

```
switchxxxxxx(config)# interface gi1/1/7
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport forbidden vlan add 234-256
```

30.31 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 gi1/1/1
Port gi1/1/1:
Port Mode: Trunk
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 2
Protected: Enabled, Uplink is gi1/1/9.
Port gi1/1/1 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 gi1/1/2
Port gi1/1/2:
VLAN Membership mode: General
Operating Parameters:
PVID: 4095 (discard vlan)
Ingress Filtering: Enabled
Acceptable Frame Type: All
GVRP status: Enabled
Protected: Disabled
Port gi1/1/1 is member in:
VLAN   Name         Egress Rule Type
----   ---------    ----------- -----
91     IP Telephony   tagged    Static
Protected: Disabled
Port gi1/1/2 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 gi1/1/2
Port gi1/1/2:
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:
```

30.32 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 gi1/1/1
Protected: Enabled, Uplink is gi1/1/1
Classification rules:
Classification Type   Group ID   VLAN ID
-------------------   --------   -------
Protocol                   1        19
Protocol                   1        20
Protocol                   2        72
Subnet                     1        15
MAC                        6        11
```

30.33 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 gi1/1/3.

```
switchxxxxxx(config)# interface gi1/1/3
switchxxxxxx(config-if)# ip internal-usage-vlan 200
```

30.34 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
--------     --------          ----------    ----------
gi1/1/21     1007              No            Active
gi1/1/22     1008              Yes           Inactive
gi1/1/23     1009              Yes           Active
```

30.35 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 `gi1/1/5` to receive Multicast transmissions from VLAN 11.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11
```

30.36 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 gi1/1/5 to receive Multicast transmissions from VLANs 5, 6, 7.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

30.37 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
------------   ----------------------
gi1/1/8,       gi1/1/1-18
gi1/1/9
```

31 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 and 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 vlan 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 gi1/1/1
```

31.5 ip igmp snooping vlan forbidden mrouter

Use the **ip igmp snooping vlan forbidden mrouter** 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 gi1/1/1
```

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
gi1/1/1
```

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 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
```

31.10 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
```

31.11 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
```

31.12 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
```

31.13 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
```

31.14 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      gi1/1/1      gi1/1/2    gi1/1/3-23
```

31.15 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 Querier is globally enabled
IGMP snooping querier global address: 194.10.12.56
IGMP Snooping Querier election is 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
```

31.16 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.

31.17 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
```

31.18 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 vlan mrouter

Use the **ipv6 mld snooping vlan 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 vlan mrouter

Use the **ipv6 mld snooping vlan mrouter** Interface 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

Interface 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 and for a range of ports as shown in the example.

Example

```
switchxxxxxx(config)interface gi1/1/1/1/1
switchxxxxxx(config-if)# ipv6 mld snooping vlan 1 mrouter interface
gi1/1/1/1/1 - 10
```

32.6 ipv6 mld snooping vlan forbidden mrouter

Use the **ipv6 mld snooping vlan forbidden mrouter** 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 gi1/1/1
```

32.7 ipv6 mld snooping vlan static

Use the **ipv6 mld snooping vlan 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 gi1/1/1
```

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-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
```

32.11 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
```

32.12 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   gi1/1/1   gi1/1/2       gi1/1/3-23
```

32.13 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
```

32.14 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 show ipv6 mld snooping groups.

```
switchxxxxxx# show ipv6 mld snooping groups

VLAN   Group Address      Source Address              Include      Exclude      Compatibility
----   --------           ---------------------       Ports        Ports        Mode
1      FF12::3            FE80::201:C9FF:FE40:8001    -----------  ----------   ---------------
1      FF12::3            FE80::201:C9FF:FE40:8002    gi1/1/1                   1
19     FF12::8            FE80::201:C9FF:FE40:8003    gi1/1/2                   1
19     FF12::8            FE80::201:C9FF:FE40:8004    gi1/1/9                   2
19     FF12::8            FE80::201:C9FF:FE40:8005    gi1/1/1      gi1/1/2      2
                                                      gi1/1/10-    gi1/1/3      2
                                                      11

MLD Reporters that are forbidden statically:

VLAN   Group Address      Source Address              Ports
----   -----------        ---------------------       --------
1      FF12::3            FE80::201:C9FF:FE40:8001    gi1/1/8
19     FF12::8            FE80::201:C9FF:FE40:8001    gi1/1/9
```

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 gi1/1/6.

```
switchxxxxxx(config)# interface gi1/1/6
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 gi1/1/6.

```
switchxxxxxx(config)# interface gi1/1/6
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 gi1/1/1.

```
switchxxxxxx# show lacp ethernet gi1/1/1

Port gi1/1/1 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 gi1/1/1 LACP Statistics:
LACP PDUs sent:                          2
LACP PDUs received:                      2

Port gi1/1/1 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 gi1/1/6.

```
switchxxxxxx(config)# interface gi1/1/6
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 `gi1/1/6` to 900 milliseconds.

```
switchxxxxxx(config)# interface gi1/1/6
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 `gi1/1/3`.

```
switchxxxxxx(config)# interface gi1/1/3
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 `gi1/1/2`.

```
switchxxxxxx(config)# interface gi1/1/2
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 `gi1/1/5`.

```
switchxxxxxx# clear gvrp statistics gi1/1/5
```

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* **|** ***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.

Default Configuration

All GVRP statistics are displayed for all interfaces. If detailed is not used, only present ports 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(s) GVRP-Status  Regist-    Dynamic          Timers(ms)
                     ration     VLAN Creation    Join   Leave   Leave All
----    ----------- --------   -------------    ----    -----   ----------
gi1/1/1     Enabled     Forbidden   Disabled         600     200    10000
gi1/1/2     Enabled     Normal      Enabled          1200    400    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
-----    ----   ----   ----   ----   ----   ----    ----   ----   ----   ----   ----   ---
gi1/1/1  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/2  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/3  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/4  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/5  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/6  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/7  0      0      0      0      0      0       0      0      0      0      0      0
gi1/1/8  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
-------- ------- ------- ------- ------- --------
 gi1/1/1      0       0       0       0       0
 gi1/1/2      0       0       0       0       0
 gi1/1/3      0       0       0       0       0
 gi1/1/4      0       0       0       0       0
 gi1/1/5      0       0       0       0       0
 gi1/1/6      0       0       0       0       0
 gi1/1/7      0       0       0       0       0
 gi1/1/8      0       0       0       0       0
```

35 Voice VLAN Commands

35.1 voice vlan state

The **voice vlan state** Global Configuration mode command sets the type of voice VLAN that is functional on the device or disables voice VLAN entirely.

The **no** format of the command returns to the default.

Syntax

voice vlan state {***oui-enabled*** | ***disabled*****]**

no voice vlan state

Parameters

- **oui-enabled**—Voice VLAN is of type OUI.
- **disabled**—Voice VLAN is disabled.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

If the administrative state is:

- **disabled** —The operational state is **disabled**.
- **oui-enabled** —The operational state is **oui-enabled**.

The following example enables the OUI mode of Voice VLAN. The first try did not work - it was necessary to first disable voice VLAN.

```
switchxxxxxx(config)# voice vlan state oui-enabled
Disable the voice VLAN before changing the voice VLAN trigger.
switchxxxxxx(config)#voice vlan state disabled
switchxxxxxx(config)#voice vlan state oui-enabled
<CR>
```

35.2 voice vlan id

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 35 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
```

35.3 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
```

35.4 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
```

35.5 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
```

35.6 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
```

35.7 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 gi1/1/2.

```
switchxxxxxx(config)# interface gi1/1/2
switchxxxxxx(config-if)# voice vlan enable
```

35.8 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 gi1/1/8.

```
switchxxxxxx(config)# interface gi1/1/8
switchxxxxxx(config-if)# voice vlan secure
```

35.9 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*] [*interface-id* **| *detailed*]**

Parameters

- **type oui**—Common and OUI-voice-VLAN specific parameters are displayed.
- **interface-id**—Specifies an Ethernet port ID. Relevant only for the OUI type.
- **detailed**—Displays information for non-present ports in addition to present ports. Only valid when type is oui.

Default Configuration

If the **type** parameter is omitted the current Voice VLAN type is used.

If the **interface-id** parameter is omitted then information about all interfaces is displayed.

All ports are displayed. If detailed is not used, only present ports are 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.

:

The following example displays the voice VLAN parameters.

```
switch>show voice vlan
Administrate Voice VLAN state is oui-enabled
The Operational Voice VLAN-ID is 2
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 mode (Ethernet port or Port-channel)

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 port gi1/1/6.

```
Console(config)# interface gi1/1/6
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 **base-mac-addr**.

```
Console(config)# loopback-detection mode base-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* **| 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. If this is not set, the default is to display all present ports.

Default Configuration

All ports are displayed. If detailed is not used, only present ports are displayed.

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
---------     ------------------
gi1/1/1       Enabled
gi1/1/2       Enabled
gi1/1/3       Disabled
gi1/1/4       Disabled
gi1/1/5       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

Parameters

N/A

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

Parameters

N/A

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 gi1/1/5 as trusted for DHCP Snooping.

```
Console(config)# interface gi1/1/5
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

Parameters

N/A

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

Parameters

N/A

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**—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.
- **expiry**
  - *seconds*—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967295)
  - ***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.

The user can add static entry to the DHCP Snooping database by using the command **ip source-guard binding**.

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 gi1/1/5
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

Parameters

N/A

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
----------- ------------
gi1/1/1         Yes
gi1/1/2         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       gi1/1/21
0060.704C.7BC1   10.1.8.2    92332     snooping    3       gi1/1/22
                                       (s)
```

37.12 ip source-guard

Use the **ip source-guard** command in Configuration mode to enable IP Source Guard globally on a device or in Interface Configuration (Ethernet, Port-channel) mode to enable IP Source Guard on an interface.

Use the **no** form of this command to disable IP Source Guard on the device or on an interface.

Syntax

ip source-guard

no ip source-guard

Parameters

N/A

Default Configuration

IP source guard is disabled.

Command Mode

Configuration or 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 `gi1/1/5`.

```
Console(config)# interface gi1/1/5
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
gi1/1/5
```

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

Parameters

N/A

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
---------                  -------
gi1/1/21                   Enabled
gi1/1/22                   Enabled
gi1/1/23                   Enabled
gi1/1/24                   Enabled
gi1/1/32                   Enabled
gi1/1/33                   Enabled
gi1/1/34                   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
-------     -----    -------    -----------      ---------------      ---    -----
gi1/1/21    IP       Active     10.1.8.1         0060.704C.73FF       3      DHCP
gi1/1/22    IP       Active     10.1.8.2         0060.704C.7BC1       3      DHCP
gi1/1/23    IP       Active     10.1.12.2        0060.704C.7BC3       4      DHCP
gi1/1/24    IP       Active     Deny all
gi1/1/25    IP       Active     10.1.8.218       0060.704C.7BAC       3      Static
gi1/1/32    IP       Inactive   10.1.8.32        0060.704C.83FF       3      DHCP
gi1/1/33    IP       Inactive
gi1/1/34    IP       Inactive
gi1/1/35    IP       Inactive
```

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

Parameters

N/A

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
--------     -----    ---------   -----------   -----   ----     ----------
gi1/1/32     IP       10.1.8.32   0060.704C.8   3       DHCP     Resource
gi1/1/33     IP                   3FF                            Problem
gi1/1/34     I                                                   Trust port
                                                                 No snooping
                                                                 VLAN
```

37.19 show ip source-guard statistics

Use the **show ip source-guard statistics** EXEC mode command to display the Source Guard dynamic information (permitted stations).

Syntax

show ip source-guard statistics [***vlan*** *vlan-id*]

Parameters

vlan-id—Display the statistics on this VLAN.

Command Mode

EXEC mode

Example

console#s**how ip source-guard statistics**

```
VLAN  Statically Permitted Stations  DHCP Snooping Permitted Stations
---- ------------------------------- --------------------------------
2      2                             3
```

37.20 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

Parameters

N/A

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
```

37.21 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
```

37.22 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

Parameters

N/A

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 gi1/1/3 as a trusted interface.

```
Console(config)# interface gi1/1/3
Console(config-if)# ip arp inspection trust
```

37.23 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

Parameters

N/A

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
```

37.24 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)#
```

37.25 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
```

37.26 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
```

37.27 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
```

37.28 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
----------- -----------
gi1/1/1          Yes
gi1/1/2          Yes
```

37.29 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

Parameters

N/A

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
```

37.30 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
```

37.31 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 DHCP Relay Commands

38.1 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
```

38.2 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
```

38.3 ip dhcp relay address (Global)

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 the server 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

User Guidelines

Use the **ip dhcp relay address** command to define a global DHCP Server IP address. To define a few DHCP Servers, use the command a few times.

To remove a DHCP Server, use the **no** form of the command with the *ip-address* argument.

The **no** form of the command without the *ip-address* argument deletes all global defined DHCP servers.

Example

The following example defines the DHCP server on the device.

```
switchxxxxxx(config)# ip dhcp relay address 176.16.1.1
```

38.4 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
```

38.5 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
```

39 IP Addressing Commands

39.1 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*]

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 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 32 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
```

39.2 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 `gi1/1/16` from DHCP.

```
switchxxxxxx(config)# interface gi1/1/16
switchxxxxxx(config-if)# ip address dhcp
```

39.3 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:

- 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
```

39.4 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
```

39.5 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.

```
switchxxxxxx# show ip interface
 IP Address        I/F          Type      Status
-------------------     ------------- ----------- -----------
10.5.234.207/24     vlan 1      Static      Valid
192.168.105.85/24 vlan 1      DHCP      Valid
```

39.6 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 gi1/1/6
```

39.7 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.

Command Mode

Global Configuration mode

Example

The following example configures the ARP timeout to 12000 seconds.

```
switchxxxxxx(config)# arp timeout 12000
```

39.8 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
```

39.9 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

This 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
```

39.10 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
```

39.11 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
```

39.12 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    gi1/1/1      10.7.1.102   00:10:B5:04:DB:4B   Dynamic
VLAN 1    gi1/1/2      10.7.1.135   00:50:22:00:2A:A4   Static
```

39.13 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)
```

39.14 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)#
```

39.15 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
```

39.16 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
```

39.17 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
```

39.18 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
```

39.19 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.

Syntax

source-precedence

no source-precedence

Default Configuration

Source precedence is not defined for the address.

Command Mode

IP Interface Configuration mode

User Guidelines

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
```

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 number.

Default Configuration

N/A

Command Mode

Global Configuration mode

Example

The following example enters the Interface Configuration (Tunnel) mode.

```
interface tunnel 1
  tunnel source auto
exit
```

40.2 tunnel destination

Use the **tunnel destination** command in Tunnel Interface Configuration mode to specify the destination for the manual tunnel interface. To remove the destination, use the **no** form of this command.

Syntax

tunnel destination {*host-name* | *ip-address*}

no tunnel destination

Parameters

- **host-name**—DNS name of the remote host.
- **ip-address**—IPv4 address of the remote host.

Default Configuration

No tunnel interface destination is specified.

Command Mode

Tunnel Interface Configuration

User Guidelines

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address.

Example

The following example shows how to configure the tunnel destination address for Manual IPv6 tunnel:

```
interface vlan 1
  ip address 10.0.0.1 255.255.255.0
exit
interface tunnel1
  ipv6 address 3ffe:b00:c18:1::3/127
  tunnel source vlan1
  tunnel destination 192.168.30.1
  tunnel mode ipv6v6ip
exit
```

40.3 tunnel mode ipv6ip

Use the **tunnel mode ipv6ip** command in Interface Configuration mode to configure a static IPv6 tunnel interface. To remove an IPv6 tunnel interface, use the **no** form of this command.

Syntax

tunnel mode ipv6ip

no tunnel mode ipv6ip

Default Configuration

IPv6 tunnel interfaces are not configured.

Command Mode

Tunnel Interface Configuration

User Guidelines

IPv6 tunneling consists of encapsulating IPv6 packets within IPv4 packets for transmission across an IPv4 routing infrastructure.

Using this command without keywords specifies an IPv6 configured tunnel where a manually-configured IPv6 address is configured on a tunnel interface and manually-configured IPv4 addresses are configured as the tunnel source and the tunnel destination. The host or router at each end of an IPv6 configured tunnel must support both the IPv4 and IPv6 protocol stacks.

Example

The following configures a manual IPv6 tunnel. In the example, tunnel interface 1 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured:

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* | *interface-id*}

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
- **interface-id**—Interface which the minimum IPv4 address is used as the source address for packets sent on the tunnel interface. If the minimum IPv4 address is removed from the interface (removed at all, moved to another interface) then the next minimum IPv4 address is chosen as the local IPv4 address.

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.

Note. If the node is an IPv4 router (IPv4 Forwarding is enabled) it strongly recommends to use an IPv4 address defined on a loopback interface as the tunnel source address. For example:

tunnel source loopback 1

Example

```
interface tunnel 1
  tunnel source auto
exit
```

40.5 show ipv6 tunnel

Use the **show ïpv6 tunnel** EXEC mode command to display tunnel information.

Syntax

show ïpv6 tunnel [**all**]

Parameters

all—The switch displays all parameters of the tunnel. If the keyword is not configured only the tunnel parameters corresponding to its type are displayed.

Command Mode

EXEC mode

Example

The following example displays information for tunnel1:

```
switchxxxxxx#  show ipv6 tunnel1
Tunnel 1
  Tunnel type                         : Manual
  Tunnel status                       : UP
  Tunnel Local address type           : VLAN 100
  Tunnel Local Ipv4 address           : 192.1.3.4
  Tunnel Remote Ipv4 address          : 192.3.4.5
Tunnel 2
  Tunnel type                         : Manual
  Tunnel status                       : DOWN
  Tunnel Local address type           : auto
  Manual parameters
    Tunnel Remote Ipv4 address        : 0.0.0.0
```

41 DHCP Server Commands

41.1 ip dhcp server

Use the **ip dhcp server** Global Configuration mode command to enable the 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
```

41.2 ip dhcp pool host

Use the **ip dhcp pool host** Global Configuration mode command to configure a 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)#
```

41.3 ip dhcp pool network

Use the **ip dhcp pool network** Global Configuration mode command to configure a 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)#
```

41.4 address (DHCP Host)

Use the **address** DHCP Pool Host Configuration mode command to manually bind an IP address to a 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

No address are bound.

Command Mode

DHCP Pool Host Configuration mode

Example

The following example manually binds an IP address to a DHCP client.

```
Console(config-dhcp)# address 10.12.1.99 255.255.255.0 01b7.0813.8811.66
```

41.5 address (DHCP Network)

Use the **address** DHCP Pool Network Configuration mode command to configure the subnet number and mask for a DHCP address pool on a 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 DHCP address pool on a DHCP server.

```
Console(config-dhcp)# address 10.12.1.0 255.255.255.0
```

41.6 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 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
```

41.7 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 Configuration

No client name is defined.

Example

The following example defines the string **client1** as the client name.

```
Console(config-dhcp)# client-name client1
```

41.8 default-router

Use the **default-router** DHCP Pool Configuration mode command to configure the default router list for a 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
```

41.9 dns-server

Use the **dns-server** DHCP Pool Configuration mode command to configure the Domain Name System (DNS) IP servers available to a 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
```

41.10 domain-name

Use the **domain-name** DHCP Pool Configuration mode command to specify the domain name for a 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
```

41.11 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 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
```

41.12 netbios-node-type

Use the **netbios-node-type** DHCP Pool Configuration mode command to configure the NetBIOS node type for Microsoft 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
```

41.13 next-server

Use the **next-server** DHCP Pool Configuration mode command to configure the next server (siaddr) in the boot process of a DHCP client. The client will connect, using SCP/TFTP, to this server in order to download the bootfile.

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
```

41.14 next-server-name

Use the **next-server-name** DHCP Pool Configuration mode command to configure the next server name (sname) in the boot process of a DHCP client. The client will connect, using SCP/TFTP, to this server in order to download the bootfile.

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
```

41.15 bootfile

Use the **bootfile** DHCP Pool Configuration mode command to specify the default boot image file name for a 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
```

41.16 time-server

Use the **time-server** DHCP Pool Configuration mode command to specify the time servers list for a 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 time server's 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
```

41.17 option

Use the **option** DHCP Pool Configuration mode command to configure the 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
```

41.18 ip dhcp excluded-address

Use the **ip dhcp excluded-address** Global Configuration mode command to specify the IP addresses that a 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
```

41.19 ip dhcp ping enable

Use the **ip dhcp ping enable** Global Configuration mode command to enable the 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
```

41.20 ping enable

Use the **ping enable** DHCP Pool Network Configuration mode command to enable the 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
```

41.21 ip dhcp ping count

Use the **ip dhcp ping count** Global Configuration mode command to specify the number of packets a 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 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
```

41.22 ip dhcp ping timeout

Use the **ip dhcp ping timeout** Global Configuration mode command to specify the time interval during which a DHCP server waits for a ping reply from an address pool.

Use the **no** form of this command to restore the default time out.

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
```

41.23 clear ip dhcp binding

The **clear ip dhcp binding** Privileged EXEC mode command deletes the dynamic address binding from the 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 supplied 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
```

41.24 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.
```

41.25 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
```

41.26 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

Example 1. The following example displays configuration of all DHCP host pools:

```
console# show ip dhcp pool host
The number of host pools is 1

Name        IP Address  Hardware Address   Client Identifier
----------  ----------  ----------------   -----------------
station     172.16.1.11                    01b7.0813.8811.66
```

Example 2. The following example displays the DHCP pool host configuration with name **station**:

```
console# show ip dhcp pool host station

Name        IP Address  Hardware Address   Client Identifier
----------  ----------  ----------------   -----------------
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
---------------------
2    3600
14   qq/aaaa/bbb.txt
19   false
```

```
21   134.14.14.1
31   1.1.1.1, 12.23.45.2
47   02af00aa00
```

41.27 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

The following example displays configuration of all DHCP network pools:

```
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
---   ------------------
2    3600
14     qq/aaaa/bbb.txt
19     false
21     134.14.14.1
31     1.1.1.1, 12.23.45.2
47     02af00aa00
```

41.28 show ip dhcp binding

Use the **show ip dhcp binding** EXEC mode command to display the specific address binding or all the address bindings on the DHCP server.

Syntax

show ip dhcp binding [*ip-address***]**

Parameters

ip-address—Specifies the IP address

Command Mode

EXEC mode

Examples

The following examples display 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
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
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.

41.29 show ip dhcp server statistics

Use the **show ip dhcp server statistics** EXEC command to display 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
```

41.30 show ip dhcp allocated

Use the **show ip dhcp allocated** EXEC mode command to display the allocated address or all the allocated addresses on the 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.

41.31 show ip dhcp declined

Use the **show ip dhcp declined** EXEC command to display the specific declined address or all of the declined addresses on the 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
```

41.32 show ip dhcp expired

Use the **show ip dhcp expired** EXEC command to display the specific expired address or all of the expired addresses on the 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
```

41.33 show ip dhcp pre-allocated

Use the **show ip dhcp pre-allocated** EXEC command to display the specific pre-allocated address or all the pre-allocated addresses on the 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
```

42 ACL Commands

42.1 ip access-list (IP extended)

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)#
```

42.2 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). Use the no form of the command to remove the access control entry.

Syntax

permit *protocol {***any** *| source source-wildcard} {***any** *| destination destination-wildcard} [***dscp** *number |* **precedence** *number]*

permit *icmp {***any** *| source source-wildcard} {***any** *| destination destination-wildcard} [***any** *| icmp-type] [***any** *| icmp-code]] [***dscp** *number |* **precedence** *number]*

permit *igmp {***any** *| source source-wildcard} {***any** *| destination destination-wildcard}[igmp-type] [***dscp** *number |* **precedence** *number]*

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]*

permit udp *{***any** *| source source-wildcard} {***any***|source-port/port-range} {***any** *| destination destination-wildcard} {***any***|destination-port/port-range} [***dscp** *number |* **precedence** *number]*

no permit *protocol {***any** *| source source-wildcard} {***any** *| destination destination-wildcard} [***dscp** *number |* **precedence** *number]*

no permit *icmp {***any** *| source source-wildcard} {***any** *| destination destination-wildcard} [***any** *| icmp-type] [***any** *| icmp-code]] [***dscp** *number |* **precedence** *number]*

no permit *igmp {***any** *| source source-wildcard} {***any** *| destination destination-wildcard}[igmp-type] [***dscp** *number |* **precedence** *number]*

no 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]*

no permit udp *{***any** *| source source-wildcard} {***any***|source-port/port-range} {***any** *| destination destination-wildcard} {***any***|destination-port/port-range} [***dscp** *number |* **precedence** *number]*

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.

Default Configuration

No IPv4 access list is defined.

Command Mode

IP Access-list Configuration mode

User Guidelines

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 any
```

42.3 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). Use the no form of the command to remove the access control entry.

Syntax

deny *protocol {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**dscp** number | **precedence** number]*

deny *icmp {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**any** | icmp-type] [**any** | icmp-code]] [**dscp** number | **precedence** number]*

deny *igmp {**any** | source source-wildcard} {**any** | destination destination-wildcard}[igmp-type] [**dscp** number | **precedence** number]*

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]*

deny udp *{**any** | source source-wildcard} {**any**|source-port/port-range} {**any** | destination destination-wildcard} {**any**|destination-port/port-range} [**dscp** number | **precedence** number]*

no deny *protocol {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**dscp** number | **precedence** number]*

no deny *icmp {**any** | source source-wildcard} {**any** | destination destination-wildcard} [**any** | icmp-type] [**any** | icmp-code]] [**dscp** number | **precedence** number]*

no deny *igmp {**any** | source source-wildcard} {**any** | destination destination-wildcard}[igmp-type] [**dscp** number | **precedence** number]*

no 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]*

no deny udp *{***any** | *source source-wildcard} {***any**|*source-port/port-range} {***any** | *destination destination-wildcard} {***any**|*destination-port/port-range} [***dscp** *number* | **precedence** *number]*

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.
- **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

The number of TCP/UDP ranges that can be defined in ACLs is limited. 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 any
```

42.4 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
```

42.5 permit (IPv6)

Use the **permit** command in IPv6 Access-list Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

permit _protocol {**any** |{source-prefix/length}{**any** | destination- prefix/length} [**dscp** number | **precedence** number]_

permit icmp _{**any** | {source-prefix/length}{**any** | destination- prefix/length} {**any**|icmp-type} {**any**|icmp-code} [**dscp** number | **precedence** number]_

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]_

permit _udp {any | {source-prefix/length}} {any | source-port/port-range}}{any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number]_

no permit _protocol {**any** |{source-prefix/length}{**any** | destination- prefix/length} [**dscp** number | **precedence** number]_

no permit icmp _{**any** | {source-prefix/length}{**any** | destination- prefix/length} {**any**|icmp-type} {**any**|icmp-code} [**dscp** number | **precedence** number]_

no 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]_

no permit _udp {any | {source-prefix/length}} {any | source-port/port-range}}{any | destination-prefix/length} {any| destination-port/port-range} [dscp number | precedence number]_

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.

Default Configuration

No IPv6 access list is defined.

Command Mode

Ipv6 Access-list Configuration mode

User Guidelines

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.

The number of TCP/UDP ranges that can be defined in ACLs is limited. 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
```

42.6 deny (IPv6)

Use the **deny** command in IPv6 Access List Configuration mode to set permit conditions (ACEs) for IPv6 ACLs. Use the no form of the command to remove the access control entry.

Syntax

deny ***protocol*** *{**any** | {source-prefix/length}{**any** | destination- prefix/length} [**dscp** number |* ***precedence*** *number][**disable-port** | **log-input**]*

deny ***icmp*** *{**any** | {source-prefix/length}{any | destination- prefix/length} {**any**|icmp-type} {**any**|icmp-code} [**dscp** number |* ***precedence*** *number]* ***[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*][***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*][***disable-port*** | ***log-input***]

no deny ***protocol*** {***any*** | *{source-prefix/length}*{***any*** | *destination- prefix/length*} [***dscp*** *number* | ***precedence*** *number*][***disable-port*** | ***log-input***]

no deny ***icmp*** {***any*** | *{source-prefix/length}{any* | *destination- prefix/length*} {***any***|*icmp-type*} {***any***|*icmp-code*} [***dscp*** *number* | ***precedence*** *number*][***disable-port*** | ***log-input***]

no 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*][***disable-port*** | ***log-input***]

no deny ***udp*** {***any*** | *{source-prefix/length}*} {***any*** | *source-port/port-range*}}{***any*** | *destination-prefix/length*} {***any***| *destination-port/port-range*} [***dscp*** *number* | ***precedence*** *number*][***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.
- **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. 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
```

42.7 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
```

42.8 permit (MAC)

Use the **permit** command in MAC Access List Configuration mode to set permit conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

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]*

no 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]*

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.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

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
```

42.9 deny (MAC)

Use the **deny** command in MAC Access List Configuration mode to set deny conditions (ACEs) for a MAC ACL. Use the no form of the command to remove the access control entry.

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] [**disable-port** | **log-input**]*

no 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] [**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.
- **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

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
```

42.10 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]* **default-action** *[**deny-any** **|** **permit-any**]*

no service-acl input

Parameters

- **acl-name**—Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).
- **deny-any**—Deny all packets (that were ingress at the port) that do not meet the rules in this ACL.
- **permit-any**—Forward all packets (that were ingress at the port) that do not meet the rules in this ACL.

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 gi1/1/1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

42.11 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 is from 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 and IPv6 ACLs 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 gi1
switchxxxxxx(config-if)# service-acl output server
```

42.12 time-range

Use the **time-range** Global Configuration mode command to define time ranges for functions . 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 adding the name of a time range with this 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
console(config-time-range)#periodic mon 12:00 to wed 12:00
```

42.13 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 http-allowed
switchxxxxxx(config-time-range)# absolute start 12:00 1 jan 2005
switchxxxxxx(config-time-range)# absolute end 12:00 31 dec 2005
```

42.14 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: mon, tue, wed, thu, fri, sat, and sun.
- **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 http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```

42.15 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 end  12:00 31 Dec 2005
periodic Monday 12:00 to Wednesday 12:00
```

42.16 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

Parameters

- **name**—Specifies the name of the ACL.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#show access-lists
Standard IP access list 1
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any
permit 234 172.30.23.8 0.0.0.255 any
```

42.17 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

```
Interface              ACLs
---------      -----------------------
gi1/1/1            blockcdp, blockvtp
gi1/1/2            Ingress: server1
               Egress : ip
```

42.18 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 gi1/1/1
```

42.19 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
---------             -------------
gi1/1/1                   79
gi1/1/2                   9
gi1/1/3                   0
Number of hits that were counted in global counter (due to lack of resources) =19
```

43 Quality of Service (QoS) Commands

43.1 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
```

43.2 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
```

43.3 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
```

43.4 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

- ***c*lass-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
```

43.5 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
Class Map matchAny class1
   Match access-group mac
```

43.6 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
```

43.7 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)#
```

43.8 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
```

43.9 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
```

43.10 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 cos-dscp
```

43.11 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: 0–7)

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
```

43.12 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: 3–10485760)
- **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
```

43.13 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
```

43.14 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
```

43.15 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
```

43.16 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
```

43.17 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

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
```

43.18 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 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)#priority-queue out num-of-queues 0
switchxxxxxx(config)#wrr-queue bandwidth 6 6 6 6 6 6 6 6
```

43.19 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
```

43.20 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 gi1/1/5 when the average traffic rate exceeds 64 kbps or the normal burst size exceeds 4096 bytes.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# traffic-shape 64 4096
```

43.21 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: 1-8)

- **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 gi1/1/5 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# traffic-shape queue 1 64 4096
```

43.22 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 (3 to maximum port speed). 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 gi1/1/5 to 150,000 kbps.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# rate-limit 150000
```

43.23 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.

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
```

43.24 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)#
```

43.25 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
```

43.26 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 gi1/1/1
gi1/1/1
Notify Q depth:
buffers gi1/1/1
Ethernet gi1/1/1
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 gi1/1/1
gi1/1/1
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 **show qos interface policer**

```
switchxxxxxx#  show qos interface policer gi1/1/1
Ethernet gi1/1/1
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 **show qos interface rate-limit**

```
console#show qos interface rate-limit gi0/1

   Port    rate-limit [kbps] Burst [Bytes]
---------- ----------------- -------------
```

```
gi0/1      3000       3000
```

```
switchxxxxxx#  show qos interface rate-limit gi1/1/1

Port          rate-limit [kbps]        Burst [Bytes]
-----         -----------------        --------------
gi1/1/1       1000                     512
```

43.27 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
```

43.28 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
```

43.29 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
```

43.30 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
```

43.31 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
```

43.32 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
```

43.33 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 gi1/1/15 to the default trust state.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# qos trust
```

43.34 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: 0–7)

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 gi1/1/5 default CoS value as 3.

```
switchxxxxxx(config)# interface gi1/1/5
switchxxxxxx(config-if)# qos cos 3
```

43.35 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

Disabled

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
```

43.36 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
```

43.37 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

43.38 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
```

43.39 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.

```
console(config)#interface gi1/1/1
switchxxxxxx(config-if)# qos statistics policer policy1 class1
```

43.40 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
```

43.41 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
```

43.42 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
gi1/1/1     Policy1     Class1     7564575          52
gi1/1/1     Policy1     Class2     8759             3214
gi1/1/2     Policy1     Class1     746587458        23
gi1/1/2     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
---------   -----       --         -------------    -----------
gi1/1/1     2           High       799921           1.2%
gi1/1/2     All         High       5387326          0.2%
```

43.43 set vlan

Use the **set vlan** Policy-map Class Configuration mode command to set a specific VLAN tag to a matched packet.

This command is only available when QoS is in advanced mode.

Syntax

set vlan *vlan-id*

no set

Parameters

- **vlan** *vlan-id*—Specifies the new VLAN ID that will be added to the traffic.

Command Mode

Policy-map Class Configuration mode

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and sets the VLAN value in the packet to VLAN 2 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 vlan 2
```

43.44 send

Use the **send** Policy-map Class Configuration mode command to send matched packets to specific target.

This command is only available when QoS is in advanced mode.

send {***copy-to-evaluation*** | ***to-all-interfaces*** | ***to-eval-and-out-port*** [port-id] | ***to-eval-and-port-group* | *to-evaluation*** | ***to-out-port*** [*port-id*] | ***to-port-group***}

no send {*copy-to-evaluation* | ***to-all-interfaces*** | ***to-eval-and-out-port*** [port-id] | ***to-eval-and-port-group* | *to-evaluation*** | ***to-out-port*** [*port-id*] | ***to-port-group*}**

Parameters

- **copy-to-evaluation**—Packet is sent to egress interface and a copy is sent to software evaluation.
- **to-all-interfaces**—Sends the matched packet to all interfaces (flood).
- **to-eval-and-out-port**—Packet is sent to evaluation and to the specified egress port
- **to-eval-and-port-group**—Packet is sent to evaluation and to specific port-group
- **to-evaluation**—Sends the matched packet for software evaluation
- t**o-out-port** [*port-id*]—Specifies to which out port to send the matched packet.
- **to-port-group**—Packet is being sent to specific Port-group, (must be created in advance)

Command Mode

Policy Map Class Configuration mode

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and sends the matched packet to port te1/0/1 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)# send to-out-port gi1/1/1/0/1
```

44 Denial of Service (DoS) Commands

44.1 security-suite deny syn-fin

Use the **security-suite deny syn-fin** Global Configuration mode command to drop all ingressing TCP packets in which both SYN and FIN are set.

Use the **no** form of this command to permit TCP packets in which both SYN and FIN are set.

Syntax

security-suite deny syn-fin

no security-suite deny syn-fin

Default Configuration

The feature is disabled by default.

Command Mode

Global Configuration mode

Example

The following example blocks TCP packets in which both SYN and FIN flags are set.

```
switchxxxxxx(config)# security-suite deny sin-fin
```

44.2 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)#
```

44.3 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
```

44.4 security-suite dos syn-attack

Use the **security-suite dos syn-attack** Interface Configuration mode command to rate limit Denial of Service (DoS) SYN attacks. This provides partial blocking of SNY packets (up to the rate that the user specifies).

Use the **no** form of this command to disable rate limiting.

Syntax

security-suite dos syn-attack *syn-rate* {***any* |** *ip-address*} {*mask* | ***I****prefix-length*}

no security-suite dos syn-attack {***any* |** *ip-address*} {*mask* | ***I****prefix-length*}

Parameters

- **syn-rate**—Specifies the maximum number of connections per second. (Range: 199–1000)
- **any | ip-address**—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 (/).

Default Configuration

No rate limit is configured.

If **ip-address** is unspecified, the default is 255.255.255.255

If **prefix-length** is unspecified, the default is 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.

This command rate limits ingress TCP packets with "SYN=1", "ACK=0" and "FIN=0" for the specified destination IP addresses.

SYN attack rate limiting is implemented after the security suite rules are applied to the packets. The ACL and QoS rules are not applied to those packets.

Since the hardware rate limiting counts bytes, it is assumed that the size of “SYN” packets is short.

Example

The following example attempts to rate limit DoS SYN attacks on a port. 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 dos syn-attack 199 any /10
To perform this command, DoS Prevention must be enabled in the
per-interface mode.
```

44.5 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
```

44.6 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.
```

44.7 security-suite deny icmp

Use the **security-suite deny icmp** Interface Configuration (Ethernet, Port-channel) mode command to discard ICMP echo requests from a specific interface (to prevent attackers from knowing that the device is on the network).

Use the **no** form of this command to permit echo requests.

Syntax

security-suite deny icmp *{[**add** {ip-address | **any**} {mask | /prefix-length}] | [**remove** {ip-address | **any**} {mask | /prefix-length}]}*

no security-suite deny icmp

Parameters

- **ip-address** | **any**—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **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 (/).

Default Configuration

Echo requests are allowed from all interfaces.

If **mask** is not specified, it defaults to 255.255.255.255.

If **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.

This command discards ICMP packets with "ICMP type= Echo request" that ingress the specified interface.

Example

The following example attempts to discard echo requests from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
To perform this command, DoS Prevention must be enabled in the
per-interface mode.
```

44.8 security-suite deny fragmented

Use the **security-suite deny fragmented** Interface Configuration (Ethernet, Port-channel) mode command to discard IP fragmented packets from a specific interface.

Use the **no** form of this command to permit IP fragmented packets.

Syntax

security-suite deny fragmented *{[**add** {ip-address | **any**} {mask | /prefix-length}] | [**remove** {ip-address | **any**} {mask | /prefix-length}]}*

no security-suite deny fragmented

Parameters

- **ip-address | any**—Specifies the destination IP address. Use **any** to specify all IP addresses.
- **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 (/).

Default Configuration

Fragmented packets are allowed from all interfaces.

If **mask** is unspecified, the default is 255.255.255.255.

If **prefix-length** is unspecified, the default is 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.

Example

The following example attempts to discard IP fragmented packets from an interface.

```
switchxxxxxx(config)# security-suite enable global-rules-only
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
To perform this command, DoS Prevention must be enabled in the
per-interface mode.
```

44.9 show security-suite configuration

Use the **show security-suite configuration** EXEC mode command to display the security-suite configuration.

Syntax

show security-suite configuration

Command Mode

EXEC mode

Example

The following example displays the security-suite configuration.

```
switchxxxxxx# show security-suite configuration
Security suite is enabled (Per interface rules are enabled).
Denial Of Service Protect: stacheldraht, invasor-trojan,
back-office-trojan.
Denial Of Service SYN-FIN Attack is enabled
Denial Of Service SYN Attack

Interface                IP Address               SYN Rate (pps)
-----------------        --------------           --------------
gi1/1/1                  176.16.23.0\24           100

Martian addresses filtering
Reserved addresses: enabled.
Configured addresses: 10.0.0.0/8, 192.168.0.0/16
SYN filtering

Interface                IP Address               TCP port
----------------         --------------           --------------
gi1/1/2                  176.16.23.0\24           FTP

ICMP filtering

Interface                IP Address
---------------          --------------
gi1/1/2                  176.16.23.0\24

Fragmented packets filtering

Interface                IP Address
--------------           --------------
gi1/1/2s                 176.16.23.0\24
```

45 VRRP Commands

45.1 clear vrrp counters

The **clear vrrp counters** Privileged EXEC mode command clears the VRRP counters.

Syntax

clear vrrp counters [*interface-id*]

Parameters

interface-id—Interface Identifier.

Default Configuration

No description.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command without the *identifier-id* argument to clear the VRRP counters of all interfaces where Virtual routers are running.

Use the **show vrrp counters** command with the *identifier-id* argument, to clear the VRRP counters of the specified interface.

Example

The following example shows how to clear the counters of all VRRP Virtual routers running on VLAN 10:

```
clear vrrp counters vlan10
```

45.2 show vrrp

The **show vrrp** Privileged EXEC mode command displays a brief or detailed status of one or all configured VRRP virtual routers.

Syntax

show vrrp [**all** | **brief** | **interface** *interface-id*]

Parameters

- **all**—Provides VRRP virtual router information about all VRRP virtual routers, including virtual routers in a disable status.
- **brief**—Provides a summary view of the VRRP virtual router information

- **interface** *interface-id*—Interface identifier

Command Mode

Privileged EXEC mode

Example 1.

```
show vrrp
Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1
Supported version is VRRPv3
State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10(down)
Source IP address is 10.3.0.20 is down; a default Source IP address of 10.2.0.10 is applied
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 3.000 sec
Preemption enabled
Priority is 100
Master Router is 10.3.0.20 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec

Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3
State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.20, 10.5.0.20
Source IP address is 10.4.0.20(default)
Virtual MAC address is 00:00:5e:00:01:02
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
Master Router is 10.4.0.20 (local), priority is 255
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
Skew Time is 1.000 sec

Interface: VLAN 50
Virtual Router 1
Supported version is VRRPv3
State is Backup
Virtual Router name CLUSTER3
Virtual IP addresses are 10.6.0.10
Source IP address is 10.6.0.20(default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 95
Master Router is 10.6.0.10, priority is 255
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
Skew Time is 0.628 sec

Interface VLAN 400
Virtual Router 4
Supported version is VRRPv3
State is Initializing
Virtual Router name CLUSTER4
Virtual IP addresses are 10.7.0.10
Source IP address is 10.7.0.20
Virtual MAC address is 00:00:5e:00:01:03
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 150
```

Example 2.

show vrrp interface vlan10

```
Interface: VLAN 10
Virtual Router 1
Virtual Router name CLUSTER1
Supported version is VRRPv3
State is Master
Virtual IP addresses are 10.2.0.10, 10.3.0.10
Source IP address is 10.3.0.20
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 3.000 sec
Preemption enabled
Priority is 100
Master Router is 10.3.0.10 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down Interval is 10.828 sec
Interface: VLAN 10
Virtual Router 2
Supported version is VRRPv3
State is Master
Virtual Router name CLUSTER2
Virtual IP addresses are 10.4.0.10, 10.5.0.10
Source IP address is 10.4.0.10
Virtual MAC address is 00:00:5e:00:01:02
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 95
Master Router is 10.4.0.10 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down Interval is 3.629 sec
```

Example 3.

```
show vrrp brief
State (S): I - Initialize; M - Master; B - Backup
Preempt (P): Y - Yes; N - No
Interface VR  Virtual        Pri Timer P St Ver Source address        Master
              Address                            Address              Address
--------- --- -------------- --- ----- - -- --- ---------------      -----------------
ge1/0/24 254 255.255.255.255 254 40000 Y M  2   255.255.255.255        255.255.255.255
VLAN 10    1 10.2.0.10       100 3000  Y M  3   10.3.0.10             10.3.0.10
             10.3.0.10
VLAN 10    2 10.4.0.10       255 1000  Y M  3   10.4.0.10             10.4.0.10
             10.5.0.10
VLAN 50    1 10.6.0.10       95  1000  Y B   3   10.6.0.10             10.6.0.60
VLAN 400   4 10.7.0.20       150 1000  Y I   3   10.7.0.10
```

45.3 show vrrp counters

The **show vrrp counters** Privileged EXEC mode command displays the VRRP counters.

Syntax

show vrrp counters [*interface-id*]

Parameters

interface-id—Interface Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show vrrp counters** command without the *identifier-id* argument, to display the VRRP counters of all interfaces where Virtual routers are running.

Use the **show vrrp counters** command with the *identifier-id* argument, to display the VRRP counters of the specified interface.

Example

The following example display the counters of all Virtual routers defined on VLAN 100:

```
show vrrp counters vlan 100
vlan 100
 Invalid checksum: 0
 Invalid Packet Length: 0
 Invalid TTL: 0
 Invalid VRRP Packet Type: 0
 Invalid VRRP ID: 0
 Invalid Protocol Number: 0
 Invalid IP List: 0
 Invalid Interval: 0
 Invalid Authentication: 0
```

45.4 vrrp description

The **vrrp description** Interface Configuration mode command assigns a description to the VRRP virtual router. The **no** format of the command returns to the default.

Syntax

vrrp *vrid* **description** *text*

no vrrp *vrid* **description**

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **text**—Text that describes the purpose or use of the virtual router. The parameter may contain 0-160 characters.

Default Configuration

No description.

Command Mode

Ethernet port, LAG, VLAN

Example

The following example shows how to assign a VRRP description to specified VRRP virtual router

```
interface vlan 10
  vrrp 1 description router1
exit
```

45.5 vrrp ip

The **vrrp ip** Interface Configuration mode command defines an IP address of a virtual router. The **no** format of the command removes an IP address.

Syntax

vrrp *vrid* **ip** *ip-address*

no vrrp *vrid* **ip** [*ip-address*]

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **ip-address**—Virtual router's IP address.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

A virtual router comes into existence when it has one or more participating VRRP routers. To participate in a specific virtual router as a VRRP router, use **vrrp ip** to configure an existing IP interface with the identifier and the IP address(es) of the virtual router. The IP interface of the VRRP router and the virtual router must be in the same IP subnet.

A VRRP router that is the owner if the virtual router's IP address(es) is also the VRRP router real IP address at the IP interface. There is only one owner for all virtual router's IP address(es). A VRRP router participates in a virtual router when it is configured with the first virtual router's IP address and does not participate when the virtual router IP address is removed.

A virtual router entity in a VRRP router is created in the shutdown state. Use the **no vrrp shutdown** command to enable it.

To defined more than one virtual router's IP address, the command should be applied for each configured IP address.

Each VRRP router in the virtual router should be configured with the same set of IP addresses.

If the *ip-address* parameter is omitted in the **no** format of the CLI command, all the IP addresses of the virtual router are remove, leading to the virtual router entity in the VRRP router being removed too.

Example

The following example shows how to define a VRRP virtual router

```
interface vlan 10
  vrrp 1 ip 192.168.2.1
exit
```

45.6 vrrp preempt

The **vrrp preempt** Interface Configuration mode command enables Virtual Router Redundancy Protocol (VRRP) preemption. The **no** format of the command disables the preemption.

Syntax

vrrp *vrid* **preempt**

no vrrp *vrid* **preempt**

Parameters

vrid—Virtual router identifier the interface for which VRRP is being defined. The range is 1-255.

Command Mode

Ethernet port, LAG, VLAN

Default Configuration

Preemption is enabled by default.

User Guidelines

By default, the VRRP router being configured with this command will take over as Master virtual router for the group if it has a higher priority than the current master virtual router.

Note: The router that is the IP address owner will preempt, regardless of the setting of this command.

Example

The following example shows how to disable VRRP preemption to specified VRRP virtual router

```
interface vlan 10
  no vrrp 1 preempt
exit
```

45.7 vrrp priority

The **vrrp priority** Interface Configuration mode command defines Virtual Router Redundancy Protocol (VRRP) priority. The **no** format of the command returns to the default.

Syntax

vrrp *vrid* **priority** *priority*

no vrrp *vrid* **priority**

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **priority**—Virtual router priority. The range is 1-254.

Command Mode

Ethernet port, LAG, VLAN

Default Configuration

The default for owner is 255 and for non-owner it is 100.

User Guidelines

The priority of the owner cannot be changed. It is always 255.

Example

The following example shows how to set VRRP priority:

```
interface vlan 10
  vrrp 1 priority 110
exit
```

45.8 vrrp shutdown

The **vrrp shutdown** Interface Configuration mode command disables the VRRP virtual router on the interface (meaning that it changes its status to Initialize). The **no** format of the command enables the VRRP virtual router.

Syntax

vrrp *vrid* **shutdown**

no vrrp *vrid* **shutdown**

Parameters

vrid—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.

Default Configuration

Disabled.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

When a VRRP virtual router is disabled on an interface its configuration is not removed.

Example

The following example shows how to enable a specified virtual router

```
interface vlan 10
  no vrrp 1 shutdown
exit
```

45.9 vrrp source-ip

The **vrrp source-ip** Interface Configuration mode command defines a real VRRP address that will be used as the source IP address of VRRP messages. The **no** format of the command returns to the default.

Syntax

vrrp *vrid* **source-ip** *ip-address*

no vrrp *vrid* **source-ip**

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **ip-address**—VRRP router's IP address: one of IP addresses of VRRP router defined on the same interface.

Default Configuration

Lowest VRRP router's IP address defined on the interface.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

Example

The following example shows how to define source ip address to specified VRRP virtual router

```
interface vlan 10
  vrrp 1 source-ip 192.168.2.1
exit
```

45.10 vrrp timers advertise

The **vrrp timers advertise** Interface Configuration mode command defines the interval between successive advertisements by the Master VRRP virtual router. The **no** format of the command returns to the default.

Syntax

vrrp *vrid* **timers advertise [msec]** *interval*

no vrrp *vrid* **timers advertise**

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **msec**—Changes the unit of the advertisement time from seconds to milliseconds. Without the keyword, the advertisement interval is in seconds.
- **interval**—Time interval between successive advertisements. If keyword **msec** is present then the valid range is 50 to 40950 milliseconds. If keyword msec is omitted then the valid range is 1 to 40 seconds.

Command Mode

Ethernet port, LAG, VLAN

Default Configuration

1 second

User Guidelines

If the advertisement interval is configured in msec, the operation advertisement interval will be the configured advertisement interval round down to the nearest seconds for VRRP v2 and to the nearest centiseconds (10ms) for VRRP v3.

Example

The following example shows how to set VRRP timer advertise of 500 msec to specified VRRP virtual router:

```
interface vlan 10
  vrrp 1 timers advertise msec 500
exit
```

45.11 vrrp version

The **vrrp version** Interface Configuration mode command defines the supported VRRP version. The **no** format of the command returns to the default.

Syntax

vrrp *vrid* **version 2** | **3** | **2&3**

no vrrp *vrid* **version**

Parameters

- **vrid**—Virtual router identifier on the interface for which VRRP is being defined. The range is 1-255.
- **2**—VRRPv2 specified by RFC3768 is supported. Received VRRPv3 messages are dropped by the VRRP virtual router. Only VRRPv2 advertisements are sent.
- **3**—VRRPv3 specified by RFC5798 is supported without VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are dropped by the VRRP virtual router. Only VRRPv3 advertisements are sent.
- **2&3**—VRRPv3 specified by RFC5798 is supported with VRRPv2 support (8.4, RFC5798). Received VRRPv2 messages are treated by the VRRP virtual router. VRRPv3 and VRRPv2 advertisements are sent.

Default Configuration

Version 2.

Command Mode

Ethernet port, LAG, VLAN

User Guidelines

Version 2&3 is intended for upgrade scenarios and is not for permanent deployment. Please refer to VRRP 3 standard for version 2 and version 3 interoperability.

Example

The following example shows how to define VRRP version to specified VRRP virtual router

```
interface vlan 10
  vrrp 1 version 2
exit
```

46 SSH Client Commands

46.1 ip ssh-client authentication

Use the **ip ssh-client authentication** command in Global Configuration mode to define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers.

To return to default, use the **no** format of the command.

Syntax

ip ssh-client authentication {**password** | **public-key** {**rsa** | **dsa**}}

no ip ssh-client authentication

Parameters

- **password**—Username and password are used for authentication.
- **public-key rsa**—Username and RSA public key are used for authentication.
- **public-key dsa**—Username and DSA public key are used for authentication.

Default Configuration

Username and password are used for authentication by the local SSH clients.

Command Mode

Global Configuration

User Guidelines

A user can use the ip ssh-client key command to generate/configure RSA/DSA keys if SSH authentication is by public key. Otherwise, the default keys generated by the switch are used.

Example

The following example specifies that, username and public key are used for authentication:

```
switchxxxxxx(config)# ip ssh-client authentication public-key rsa
```

46.2 ip ssh-client change server password

Use the **ip ssh-client change server password** command in Global Configuration mode to change a password of an SSH client on a remote SSH server.

Syntax

ip ssh-client change server password server *{host* | *ip-address* | *ipv6-address}* **username** *username* **old-password** *old-password* **new-password** *new-password*

Parameters

- **host**—DNS name of a remote SSH server.

- **ip-address**—Specifies the IP address of a remote SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **username** —Username of the local SSH clients (1 - 70 characters).
- **old-password** —Old password of the local SSH client (1 - 70 characters).
- **new-password**—New password for the local SSH client (1 - 70 characters). The password cannot include the characters "@" and ":".

Default Configuration

N/A

Command Mode

Global configuration

User Guidelines

Use the command to change a password on a remote SSH server. Use ip ssh-client password to change the SSH client password of the switch's SSH client so that it matches the new password set on the remote SSH server.

Example

The following example changes a password of the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client change server password server
10.7.50.155 username john old-password &&&@@@aaff new-password
&&&@@@aaee
```

46.3 ip ssh-client key

Use the **ip ssh-client key** command in Global Configuration mode to create a key pair for SSH client authentication by public key (either by generating a key or by importing a key).

To remove a key, use the **no** form of the command.

Syntax

ip ssh-client key {**dsa** | **rsa**} {**generate | key-pair** *privkey pubkey***}**

no ip ssh-client key [**dsa** | **rsa**]

Parameters

- **dsa**—DSA key type.
- **rsa**—RSA key type.
- **key-pair**—Key that is imported to the device.
- **privkey**—Plaintext private key.
- —**pubkey**—The plaintext pubic key.

Default Configuration

The application creates a key automatically; this is the default key.

Command Mode

Global configuration

User Guidelines

When using the keyword **generate**, a private key and a public key of the given type (RSA/DSA) are generated for the SSH client. Downloading a configuration file with a Key Generating command is not allowed, and such download will fail.

When using the keyword **key-pair,** the user can import a key-pair created by another device. In this case, the keys must follow the format specified by RFC 4716.

If the specified key already exists, a warning will be issued before replacing the existing key with a new key.

Use the **no ip ssh-client key** command to remove a key pair. Use this command without specifying a key-type to remove both key pairs.

Table 4 describes the expected behavior of keys, default and users within the various operations.

Table 4: Keys, Defaults and Users

From/To	Show	Show (detailed)	Copy/Upload of Running Config	Copy/Upload of Startup Config	Download text-based CLI (TFTP/Backup)
Startup Config	Only user-defined.	N/A	All keys (default and user)	N/A	All keys (default and user)
Running Config	Keys are not displayed.	All keys (default and user)	N/A	Only user defined.	Same as user configuration
Text-based CLI (TFTP/Backup)	As it was copied.	N/A	All keys (default and user)	Only user defined.	As a text file.

If no keys are included in text-based configuration file, the device generates it's own keys during initialization. If the Running Configuration contains default keys (not user-defined), the same default keys remain.

Examples

Example 1 - In the following example, a key pair of the RSA type is created:

```
switchxxxxxx(config)# ip ssh-client key rsa generate
The SSH service is generating a private RSA key.
This may take a few minutes, depending on the key size.
```

Example 2 - In the following example, both public and private keys of the RSA type are imported (private key as plaintext):

```
switchxxxxxx(config)#ip ssh-client key rsa key-pair
Please paste the input now, add a period (.) on a separate line after the
input
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDH6CU/2KYRl8rYrK5+TIvwS4zvhBmiC4I31m9cR/1iRTFViMRuJ++TEr
p9ssqWyI1Ti9d0jzmG0N3jHzp2je5/DUTHZXvYaUzchBDnsPTJo8dyiBl4YBqYHQgCjUhk
tXqvloy+1uxRJTAaLVXCBAmuIU/kMLoEox8/zwjB/jsF9wIBIwKBgC2xZ5mQmvy0+yo2GU
FwlQO5f0yweuM11J8McTmqDgfVTRrdbroXwbs3exVqsfaUPY9wa8Le6JPX+DPp4XovEfC/
```

```
iglZBSC8SeDmI2U7D6HrkAyD9HHf/r32jukB+5Z7BlHPz2Xczs2clOOwrnToy+YTzjLUxy
WS7V/IxbBllipLAkEA/QluVSCfFmdMlZxaEfJVzqPO1cF8guovsWLteBf/gqHuvbHuNy0t
OWEpObKZs1m/mtCWppkgcqgrB0oJaYbUFQJBAMo/cCrkyhsiV/+ZsryeD26NbPEKiak16V
Tz2ayDstidGuuvcvm2YF7DjM6n6NYz3+/ZLyc5n82okbld1NhDONsCQQCmSAas+C4HaHQn
zSU+/lWlDI88As4qJN2DMmGJbtsbVHhQxWIHAG4tBVWa8bV12+RPyuan/jnk8irniGyVza
FPAkEAiq8oV+1XYxA8V39V/a42d7FvRjMckUmKDl4Rmt32+u9i6sFzaWcdgs87+2vS3AZQ
afQDE5U6YSMiGLVewC4YWwJBAOFZmhO+dIlxT8Irzf2cUZGggopfnX6Y+L+Yl09MuZHbwH
tXaBGj6ayMYvXnloONecnApBjGEm37YVwKjO2DV2w=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMfoJT/YphGXytisrn5Mi/BLjO+EGaILgjfWb1xH/WJFMVWIxG4n75MSun2yyp
bIjVOL13SPOYbQ3eMfOnaN7n8NRMdle9hpTNyEEOew9Mmjx3KIGXhgGpgdCAKNSGS1eq+W
jL7W7FElMBotVcIECa4hT+QwugSjHz/PCMH+OwX3AgEj
-----END RSA PUBLIC KEY-----
.
```

Example 3 - In the following example, both public and private keys of the DSA type are imported (private key as encrypted):

```
switchxxxxxx(config)# encrypted ip ssh-client key rsa key-pair
(Need to encrypted SSH client RSA key pair, for example:)
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
gxeOjs6OzGRtL4qstmQg1B/4gexQblfa56RdjgHAMejvUT02elYmNi+m4aTu6mlyXPHmYP
lXlXny7jZkHRvgg8EzcppEB0O3yQzq3kNi756cMg4Oqbkm7TUOtdqYFEz/h8rJJ0QvUFfh
BsEQ3e16E/OPitWgK43WTzedsuyFeOoMXR9BCuxPUJc2UeqQVM2IJt5OM0FbVt0S6oqXhG
sEEdoTlhlDwHWg97FcV7x+bEnPfzFGrmbrUxcxOxlkFsuCNo3/94PHK8zEXyWtrx2KoCDQ
qFRuM8uecpjmDh6MO2GURUVstctohEWEIVCIOr5SBCbciaxv5oS0jIzXMrJA==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALLOeh3css8tBL8ujFt3trcX0XJyJLlxxt4sGp8Q3ExlSRN25+Mcac6togpIEg
tIzk6t1IEJscuAih9Brwh1ovgMLRaMe25j5YjO4xG6Fp42nhHiRcie+YTS1o309EdZkiXa
QeJtLdnYL/r3uTIRVGbXI5nxwtfWpwEgxxDwfqzHAgEj
-----END RSA PUBLIC KEY-----
```

Example 4 - In the following example, a DSA key pair is removed:

```
switchxxxxxx(config)# no ip ssh-client key dsa
```

Example 5 - In the following example, all key pairs (RSA and DSA types) are removed.

```
switchxxxxxx(config)# no ip ssh-client key
```

46.4 ip ssh-client password

Use the **ip ssh-client password** command in Global Configuration mode to configure the password for SSH client authentication by password.

To return to default, use the **no** form of the command.

Syntax

ip ssh-client password *string*

no ip ssh-client password

Parameters

- **string**—Password for the SSH clients (1 - 70 characters). The password cannot include the characters "@" and ":".

Default Configuration

The default password is anonymous.

Command Mode

Global configuration

User Guidelines

If authentication is configured to use a password (using the command **ip ssh-client authentication**), use the **ip ssh-client password** command to define the password.

Use the command **ip ssh-client change server password** to change the password on the remote SSH server so that it will match the new password of the SSH client.

Example

The following example specifies a plaintext password for the local SSH clients:

```
switchxxxxxx(config)# ip ssh-client password &&&111aaff
```

46.5 ip ssh-client server authentication

Use the i**p ssh-client server authentication** command in Global Configuration mode to enable remote SSH server authentication by the SSH client.

To disable remote SSH server authentication, use the **no** form of the command.

Syntax

ip ssh-client server authentication

no ip ssh-client server authentication

Parameters

None

Default Configuration

SSH server authentication is disabled

Command Mode

Global configuration

User Guidelines

When remote SSH server authentication is disabled, any remote SSH server is accepted (even if there is no entry for the remote SSH server in the SSH Trusted Remote Server table).

When remote SSH server authentication is enabled, only trusted SSH servers are accepted. Use the ip ssh-client server fingerprint command to configure trusted SSH servers.

Example

The following example enables SSH server authentication:

```
switchxxxxxx(config)# ip ssh-client server authentication
```

46.6 ip ssh-client server fingerprint

Use the **ip ssh-client server fingerprint** command in Global configuration mode to add a trusted server to the Trusted Remote SSH Server Table. To remove an entry or all entries from the Trusted Remote SSH Server Table, use the **no** form of the command.

Syntax

ip ssh-client server fingerprint {*host* | *ip-address*} *fingerprint*

no ip ssh-client server fingerprint [*host* | *ip-address*]

Parameters

- **host**—DNS name of a SSH server.
- **ip-address**—Specifies the address of a SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.
- **fingerprint**—FIngerprint of the SSH server public key (32 Hex characters).

Default Configuration

The Trusted Remote SSH Server table is empty.

Command Mode

Global configuration

User Guidelines

Fingerprints are created by applying a cryptographic hash function to a public key. Fingerprints are shorter than the keys they refer to, making it simpler to use (easier to manually input than the original key). Whenever the switch is required to authenticate an SSH server's public key, it calculates the received key's fingerprint and compares it to the previously-configured fingerprint.

The fingerprint can be obtained from the SSH server (the fingerprint is calculated when the public key is generated on the SSH server).

The **no ip ssh-client server fingerprint** command removes all entries from the Trusted Remote SSH Server table.

Example

In the following example, a trusted server is added to the Trusted Servers table (with and without a separator ":"):

```
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC789788DC88A988127897BCBB789788
switchxxxxxx(config)# ip ssh-client server fingerprint 1.1.1.1
DC:78:97:88:DC:88:A9:88:12:78:97:BC:BB:78:97:88
```

46.7 ip ssh-client username

Use the **ip ssh-client username** command in Global Configuration mode to configure the SSH client username of the switch.

To return to default, use the **no** form of the command.

Syntax

ip ssh-client username *string*

no ip ssh-client username

Parameters

string—Username of the SSH client.The length is 1 - 70 characters. The username cannot include the characters "@" and ":".

Default Configuration

The default username is anonymous

Command Mode

Global configuration

User Guidelines

The configured username is used when SSH client authentication is done both by password or by key.

Example

The following example specifies a username of the SSH client:

```
switchxxxxxx(config)# ip ssh-client username jeff
```

46.8 show ip ssh-client

Use the **show ip ssh-client** command in Privilege EXEC mode to display the SSH client credentials, both default and user-defined keys.

Syntax

show ip ssh-client

show ip ssh-client {**mypubkey | key}** {**dsa** | **rsa**}

Parameters

- **dsa**—Specifies displaying the DSA key type.
- **rsa**—Specifies displaying the RSA key type.
- **mypubkey**—Specifies that the public key is selected to be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command with a specific key-type to display the SSH client key; You can either specify display of public key or private key, or with no parameter to display both private and public keys. The keys are displayed in the format specified by RFC 4716.

Example

Example 1 - The following example displays the authentication method and the RSA public key:

```
switchxxxxxx# show ip ssh-client mypubkey rsa
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAudGEIaPARsKoVJVjs8XALAKqBN1WmXnY
kUf5oZjGY3QoMGDvNipQvdN3YmwLUBiKk31WvVwFB3N2K5a7fUBjoblkdjns
QKTKZiu4V+IL5rds/bD6LOEkJbjUzOjmp9hlIkh9uc0ceZ3ZxMtKhnORLrXL
aRyxYszO5FuirTo6xW8=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 84:f8:24:db:74:9c:2d:51:06:0a:61:ef:82:13:88:88
```

Example 2 - The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Authentication method:   DSA key
Username:                john
Key Source:              User Defined
Public Key Fingerprint:
77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86---- BEGIN SSH2 PUBLIC KEY
----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
```

```
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

Example 3 - The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
Authentication method:   DSA key
Username:                anonymous (default)
Password:                anonymous (default)
```

46.9 show ip ssh-client server

Use the **show ip ssh-client server** command in Privilege EXEC Configuration mode to display the SSH remote server authentication method and the Trusted Remote SSH Server table.

Syntax

show ip ssh--client server [*host* | *ip-address*]

Parameters

- **host** —DNS name of an SSH server.
- **ip-address**—IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

N/A

Command Mode

Privilege EXEC configuration mode

User Guidelines

If a specific SSH server is specified, only the fingerprint of this SSH server is displayed. Otherwise, all known servers are displayed.

Example

Example 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:

```
switchxxxxxx# show ip ssh-client server
SSH Server Authentication is enabled
server address: 11.1.0.1
  Server Key Fingerprint: 5a:8d:1d:b5:37:a4:16:46:23:59:eb:44:13:b9:33:e9
server address: 192.165.204.111
  Server Key Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
server address: 4002:0011::12
  Server Key Fingerprint: a5:34:44:44:27:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

Example 2 - The following example displays the authentication method and DSA private key in encrypted format:

```
switchxxxxxx# show ip ssh-client key DSA
Authentication method:   DSA key
Username:                john
Key Source:              Default
Public Key Fingerprint:
77:C7:19:85:98:19:27:96:C9:CC:83:C5:78:89:F8:86---- BEGIN SSH2 PUBLIC KEY
----
Comment: RSA Public Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PUBLIC KEY ----
---- BEGIN SSH2 PRIVATE KEY ----
Comment: DSA Private Key
AAAAB3NzaC1kc3MAAACBAPY8ZOHY2yFSJA6XYC9HRwNHxaehvx5wOJ0rzZdzoSOXxbET
W6ToHv8D1UJ/z+zHo9Fiko5XybZnDIaBDHtblQ+Yp7StxyltHnXF1YLfKD1G4T6JYrdH
YI14Om1eg9e4NnCRleaqoZPF3UGfZia6bXrGTQf3gJq2e7Yisk/gF+1VAAAAFQDb8D5c
vwHWTZDPfX0D2s9Rd7NBvQAAAIEAlN92+Bb7D4KLYk3IwRbXblwXdkPggA4pfdtW9vGf
J0/RHd+NjB4eo1D+0dix6tXwYGN7PKS5R/FXPNwxHPapcj9uL1Jn2AWQ2dsknf+i/FAA
vioUPkmdMc0zuWoSOEsSNhVDtX3WdvVcGcBq9cetzrtOKWOocJmJ80qadxTRHtUAAACB
AN7CY+KKv1gHpRzFwdQm7HK9bb1LAo2KwaoXnadFgeptNBQeSXG1vO+JsvphVMBJc9HS
n24VYtYtsMu74qXviYjziVucWKjjKEb11juqnF0GDlB3VVmxHLmxnAz643WK42Z7dLM5
sY29ouezv4Xz2PuMch5VGPP+CDqzCM4loWgV
---- END SSH2 PRIVATE KEY ----
```

Example 3 - The following example displays the SSH client authentication method, the username and the password:

```
switchxxxxxx# show ip ssh-client
Authentication method: password (default)
Username: anonymous (default)
password(Encrypted): KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5
```

47 IP Routing Protocol-Independent Commands

47.1 accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the a**ccept-lifetime** command inkey chain key configuration mode. 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 date year*

hh:*mm*:*ss date Month year*

hh—hours (0-23)

mm—minutes (0-59

ss—seconds (0-59)

Month—first three letters of the month

date—date (1-31)

year—year (four digits)

The default start time and the earliest acceptable date is January 1, 2000.

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 time period during which the authentication key is valid for authenticating incoming packets is set to **Forever**.

The definition of **Forever** is: the starting time is January 1, 2000, and the ending time is infinite.

Command Mode

Key chain key configuration

User Guidelines

The switch checks **Time-of-Date** again a value of the *start-time* argument regardless if **Time-of-Date** is not set by management or by SNTP because of the default value of Time-of-Date always is an passed time.

If validation of the value of the *start-time* argument was passed and the *end-time* argument is configured and its value is **infinite** the key is considered as actual regardless if **Time-of-Date** is not set by management or by SNTP.

If **Time-of-Date** is not set by management or by SNTP and if the *end-time* argument is configured with a value differing from **infinite** or the **duration** parameter is configured, the key is considered as expired.

If **Time-of-Date** is set by management or by SNTP, the switch checks **Time-of-Date** again a value of the *end-time* argument or of the **duration** parameter.

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
```

47.2 clear ip prefix-list

The **clear ip prefix-list** Privileged EXEC mode command resets IP prefix-list counters.

Syntax

clear ip prefix-list [*prefix-list-name* [*network*/*length*]]

Parameters

prefix-list-name—Name of the prefix list from which the hit count is to be cleared.

network/length—Network number and length (in bits) of the network mask. The slash mark must precede the bit length value.

Parameters ranges

network /length—The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32.

Default Configuration

Command Mode

Privileged EXEC

User Guidelines

The **clear ip prefix-list** command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Example In the following example, the prefix-list counters are cleared for the prefix list named FIRST_LIST that matches the 10.0.0.0/8 prefix:

```
clear ip prefix-list FIRST_LIST 10.0.0.0/8
```

47.3 distance (IP)

To define an administrative distance for routes that are inserted into the routing table, use the **distance** command in global configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

Syntax

distance {**static** | **rip**} *distance*

no distance {**static** | **rip**}

distance ospf {**inter-as** | **intra-as**} *distance*

no distance ospf {**inter-as** | **intra-as**}

distance bgp {**external** | **internal** | **local**} *distance*

no distance bgp {**external** | **internal** | **local**}

Parameters

static—Administrative distance for static routes

rip—Administrative distance for RIP routes

ospf—Administrative distance for OSPF for IPv6 routes.

bgp—Administrative distance for BGP for IPv6 routes.

ospf inter-as—Administrative distance for OSPF routes from one Autonomous System to another Autonomous System (LSAs type 5 and type 7 routes, external 2 metric).

ospf intra-as—Administrative distance for OSPF routes within an Autonomous System (Internal and External 1 metric.

bgp external—Administrative distance for Border Gateway Protocol (BGP) external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.

bgp internal—Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

bgp local—Administrative distance for BGP local routes. Local routes are those networks listed with a network router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

distance—Administrative distance. An integer from 1 to 255. A value of 0 is reserved for **connected** routes that cannot be changed.

Default Configuration

static—1

rip—120

ospf intra-as—30

ospf inter-as—110

bgp external—20

bgp internal—200

bgp local—200

Command Mode

Global Configuration mode

User Guidelines

An administrative distance is a rating of the trust worthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Example

In the following example, distance 20 is set for OSPF internal routes and distance 40 is set for RIP routes:

```
distance ospf intra-as 20
distance rip 40
```

47.4 ip prefix-list

The **ip prefix-list** Global Configuration mode command creates a prefix list or adds a prefix-list entry. The **no** format of the command deletes a prefix list or a prefix-list entry.

Syntax

ip prefix-list *prefix-list-name* [**seq** *number*] {{**deny**|**permit**} *network* /*length* [**ge** *ge-length*] [**le** *le-length*]} | **description** *text*

no ip prefix-list *prefix-list-name* [**seq** *number*]

Parameters

prefix-list-name—The name of the IP prefix list. The name may contain up to 32 characters.

seq *number—*Sequence number of the prefix list entry being configured. It is an integer value from 1 to 4294967294.

deny—Denies access for a matching condition.

permit—Permits access for a matching condition.

network /**length**—Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32. The zero length may be used only with the zero network (**0.0.0.0**).

ge *ge-length—*Specifies the lesser value of a range (the "from" portion of the range description) by applying the ge-length argument to the range specified. ge-length represents the minimum prefix length to be matched.

Note. The **ge** keyword represents the greater than or equal to operator.

le l*e-length—*Specifies the greater value of a range (the "from" portion of the range description) by applying the Represents the minimum prefix length to be matched argument to the range specified. le-length represents the maximum prefix length to be matched

Note. The le keyword represents the lesser than or equal to operator.

description *text—*A comment entry with text that can be up to 80 characters in length.

Default Configuration

seq *number—*The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.

Command Mode

Global Configuration mode

User Guidelines

Use the **ip prefix-list** command to configure IP prefix filtering. Prefix lists are configured with **permit** or **deny** keywords to either permit or deny a prefix based on a matching condition. An implicit **deny** is applied to traffic that does not match any prefix-list entry.

A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number from 1 to 32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the **ge** and **le** keywords are used. The **ge** and **le** keywords are used to specify a range of prefix lengths and provide more flexible configuration than using only the *network*/*length* argument. A prefix list is processed using an exact match when neither the **ge** nor **le** keyword is specified. If only the **ge** value is specified, the range is the value entered for the **ge** *ge-length* argument to a full 32-bit length. If only the le value is specified, the range is from the value entered for the *network*/*length* argument to the **le** l*e-length* argument. If both the **ge** *ge -length* and **le** l*e-length* keywords and arguments are entered, the range is between the values used for the *ge-length* and *le-length* arguments.

The following formula shows this behavior:

length < ge ge-length < le le-length <= 32

The **ip prefix-list** command without the **seq** keyword adds the new entry after the last entry of the prefix list with the sequence number equals to the last number plus 5. For example, if the last configured sequence number is 43, the new entry will have the sequence number of 48. If the list is empty the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.

The **ip prefix-list** command with the **seq** keyword puts the new entry into the place specified by the parameter, if an entry with the number exists it is replaced by the new one.

The **no ip prefix-list** command without the **seq** keyword removes the prefix list.

The **no ip prefix-list** command with the **seq** keyword removes the specified entry.

Evaluation of a prefix list starts with the lowest sequence number and continues down the list until a match is found. When an IP address match is found, the permit or deny statement is applied to that network and the remainder of the list is not evaluated.

Use the **ip prefix-list** command with the **description** keyword to insert a comment entry into the prefix list.

Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

Formal specification

Checked prefix is **cP** and checked prefix length is **cL**.

Function **PrefixIsEqual**(P1, P2, L) compares the first L bits of two addresses P1 and P2 and returns TRUE if they are equal.

Case 1. An prefix-list entry is:

P - prefix address

L - prefix length

ge - is not defined

le - is not defined

The prefix cP/cL matches to the prefix-list entry if

PrefixIsEqual(cP,P,L) && **cL**==**L**

Case 2. An prefix-list entry is:

P - prefix address

L - prefix length

ge - is defined

le - is not defined

The prefix cP/cL matches to the prefix-list entry if

PrefixIsEqual(cP,P,L) && **cL**>=**ge**

Case 3. An prefix-list entry is:

P - prefix address

L - prefix length

ge - is not defined

le - is defined

The prefix cP/cL matches to the prefix-list entry if

PrefixIsEqual(cP,P,L) && **cL**<=**le**

Case 4. An prefix-list entry is:

P - prefix address

L - prefix length

ge - is defined

le - is defined

The prefix cP/cL matches to the prefix-list entry if

PrefixIsEqual(cP,P,L) && **ge**<=**cL**<=**le**

Example

Example 1. In the following example, a prefix list is configured to deny the default route 0.0.0.0/0:

```
ip prefix-list RED deny 0.0.0.0/0
```

Example 2. In the following example, a prefix list is configured to permit traffic from the 172.16.1.0/24 subnet:

```
ip prefix-list BLUE permit 172.16.1.0/24
```

Example 3. In the following example, a prefix list is configured to permit routes from the 10.0.0.0/8 network that have a mask length that is less than or equal to 24 bits:

```
ip prefix-list YELLOW permit 10.0.0.0/8 le 24
```

Example 4. In the following example, a prefix list is configured to deny routes from the 10.0.0.0/8 network that have a mask length that is greater than or equal to 25 bits:

```
ip prefix-list PINK deny 10.0.0.0/8 ge 25
```

Example 5. In the following example, a prefix list is configured to permit routes from any network that have a mask length from 8 to 24 bits:

```
ip prefix-list GREEN permit 0.0.0.0/0 ge 8 le 24
```

Example 6. In the following example, a prefix list is configured to deny any route with any mask length from the 10.0.0.0/8 network:

```
ip prefix-list ORANGE deny 10.0.0.0/8 le 32
```

47.5 ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

Syntax

ip route *prefix* {*mask* | **/***prefix-length*} {{*ip-address* [**metric** *cost*]} | **reject-route**}

no ip route *prefix* {*mask* | *prefix-length*} [*ip-address*]

Parameters

prefix—IP route prefix for the destination.

mask—Prefix mask for the destination.

/prefix-length—Prefix mask for the destination.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—IP address of the next hop that can be used to reach that network.

reject-route—Stops routing to the destination network via all gateways.

metric cost—Cost(metric) of the route. The default cost 1. Range: 1–255.

reject-route—Stops routing to the destination network.

Default Configuration

No static routes are established.

Command Mode

Global configuration (config)

User Guidelines

Use the **no ip route** comand without the i*p-address* parameter to remove all static routes to the given subnet.

Use the **no ip route** comand with the *ip-address* parameter to remove only one static route to the given subnet via the given next hop.

Example

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:

```
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 :

```
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:

```
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:

```
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:

```
no ip route 194.1.1.0 /24 1.1.1.1
```

47.6 ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no** form of this command.

Syntax

ip routing

no ip routing

Parameters

This command has no arguments or keywords.

Default Configuration

IP routing is disabled.

Command Mode

Global configuration (config)

User Guidelines

Example The following example enables IP routing

```
ip routing
```

47.7 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

No key exists.

Command Mode

Key chain key configuration.

User Guidelines

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
```

47.8 key (key chain)

To identify an authentication key on a key chain, use the **key** command in key-chain configuration 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, which 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 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 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 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
```

47.9 key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the **key chain** command in global configuration 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, we recommend using one key chain per interface per routing protocol. Upon specifying the key chain command, you enter **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:

```
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
```

47.10 send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. 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 date year*

hh:*mm*:*ss date Month year*

hh—hours (0-23)

mm—minutes (0-59

ss—seconds (0-59)

Month—first three letters of the month

date—date (1-31)

year—year (four digits)

The default start time and the earliest acceptable date is January 1, 2000.

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 time period during which the authentication key is valid for authenticating incoming packets is set to forever.

Forever (the starting time is January 1, 2000, 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
```

47.11 show distance

To display the distance of the IP routing protocols, use the **show distance** command in user EXEC or privileged EXEC mode.

Syntax

show distance

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the command to display the distance of the IP routing protocols

Example

The following is sample output from the **show distance** command:

```
show distance
```

```
Protocol      Distance
-------       --------
connected          0
static             1
rip              120
ospf intra-as     30
ospf inter-as    110
bgp external      20
bgp internal     200
bgp local        200
```

47.12 show ip prefix-list

The **show ip prefix-list** Privileged EXEC mode command displays information about a prefix list or prefix list entries.

Syntax

show ip prefix-list [**detail** [*list-name*] | **summary** [*list-name*]]

s**how ip prefix-list** *list-name network/length* [**longer** | **first-match**]

show ip prefix-list *list-name* **seq** *seq-num*

Parameters

detail | **summary**—Displays detailed or summarized information about prefix lists.

prefix-list-name—Displays the entries in a specific prefix list.

seq *number*—Displays only the prefix list entry with the specified sequence number in the specified prefix-list.

network/length—Displays all entries in the specified prefix list that use this network address and netmask length (in bits).

longer—Displays all entries of the specified prefix list that match or are more specific than the given network/length.

first-match—Displays the first entry of the specified prefix list that matches the given network/length.

Command Mode

Privileged EXEC mode

Default Configuration

User Guidelines

If the **detail** and **summary** keywords are omitted the **detail** option is applied.

If the **longer** and f**irst-match** keywords are omitted all entries of the specified prefix list that matches the given network/length are displayed.

Example

Example 1. The following example shows the output of the **show ip prefix-list** command with the **detail** keyword:

```
show ip prefix-list detail

ip prefix-list ABC:
  count: 1, range entries: 0
  seq 5 permit 10.0.0.0/8 (hit count: 313)
ip prefix-list aggregate:
  count: 3, range entries: 2
  seq 5 deny 192.12.25.0/24 ge 25 (hit count: 568)
  seq 10 description The Default Action
  seq 15 permit 0.0.0.0/0 le 28 (hit count: 31310)
ip prefix-list bgp-in:
  count: 6, range entries: 3
  seq 5 deny 54.0.0.0/8 le 28 (hit count: 0)
  seq 10 deny 0.0.0.0/0 (hit count: 0)
  seq 15 deny 1.0.0.0/8 (hit count: 0)
  seq 20 deny 2.0.0.0/8 (hit count: 0)
  seq 25 deny 3.1.0.0/16 ge 24 (hit count: 0)
  seq 30 permit 0.0.0.0/0 le 18 (hit count: 240664)
```

Field’s descriptions:

count—Number of entries in the list.
range entries—Number of entries with matching range.
seq—Entry number in the list.
permit, deny—Granting status.
description—Comment.
hit count—Number of matches for the prefix entry.

Example 2. The following example shows the output of the **show ip prefix-list** command with the **summary** keyword:

```
show ip prefix-list summary

ip prefix-list ABC:
  count: 1, range entries: 0
ip prefix-list aggregate:
  count: 2, range entries: 2
ip prefix-list bgp-in:
  count: 6, range entries: 3
```

Example 3. The following example shows the output of the **show ip prefix-list** command with the **seq** keyword:

```
show ip prefix-list bgp-in seq 15

  seq 15 deny 1.0.0.0/8 (hit count: 0)
```

47.13 show ip protocols

To display the parameters and current state of the active IP routing protocol processes, use the **show ip protocols** command in user EXEC or privileged EXEC mode.

Syntax

show ip protocols [**summary**]

Parameters

summary—Displays the configured routing protocol process names.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The information displayed by the show ipv6 protocols command is useful in debugging routing operations.

Example

Example 1. The following is sample output from the **show ip protocols** command, showing active routing protocols:

```
show ip protocols

IP Routing Protocol is "rip"
  Interfaces  IP Addresses
    VLAN 1    12.1.1.1
    VLAN 1    150.23.12.2
    VLAN 11   1.1.1.1
IP Routing Protocol is "ospf 1"
  Interfaces  IP Addresses
    VLAN 3    2.2.2.2
    VLAN 100  154.23.111.1
IPv6 Routing Protocol is "ospf 10"
  Interfaces IP Addresses
    VLAN 10   123.1.1.1
    VLAN 130  4.4.4.4
```

Example 2. The following is sample output from the **show ip protocols** command with the **summary** keyword:

```
show ipv6 protocols summary

IP Routing Protocol is "rip"
IP Routing Protocol is "ospf 1"
IP Routing Protocol is "ospf 10"
```

47.14 show ip route

TTo display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

Syntax

show ip route [*ip-address* {*mask* [**longer-prefixes**]} | *protocol* [*process-id*] | **static** | **rejected**]

Parameters

ip-address—IP address about which routing information should be displayed.

mask—The subnet mask.

longer-prefixes—Specifies that only routes matching the ip-address and mask pair should be displayed.

protocol—The name of a routing protocol, or the keyword connected, mobile, static, or summary. If you specify a routing protocol, use one of the following keywords: **bgp**, **ospf**, and **rip**; or displays routes for the specified type of route using any of these keywords: **connected**, **static**, or **icmp**.

process-id—The number used to identify a process of the specified protocol.

static—Displays static routes.

rejected—Displays rejected routes.

Command Mode

User EXEC (>)

Privileged EXEC (#)

User Guidelines

Example

Example 1. The following is sample output from the **show ip route** command when IP Routing is not enabled:

```
Router# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: disabled

Codes: > - best, C - connected, S - static
```

```
IP Routing Table - 5 entries
Code    IP Route        Distance/  Next Hop         Last Time Outgoing
                        Metric     IP Address       Updated   Interface
------  --------------------  -----------  ---------------  ------------- ------------
S>      10.10.0.0/16    1/128      10.119.254.244  00:02:22  ge1/0/2
S>      10.10.0.0/16    1/128      10.120.254.244  00:02:22  ge1/0/3
S>      10.16.2.0/24    1/128      10.119.254.244  00:02:22  ge1/0/2
C>      10.119.0.0/16   0/1        0.0.0.0                   ge1/0/2
C>      10.120.0.0/16   0/1        0.0.0.0                   ge1/0/3
```

Example 2. The following is sample output from the **show ip route** command when IP Routing is enabled:

```
Router# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled

Codes: > - best, C - connected, S - static,
       R - RIP,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP

IP Routing Table - 22 entries
Code    IP Route        Distance/  Next Hop         Last Time Outgoing
                        Metric     IP Address       Updated   Interface
------  --------------------  -----------  ---------------  ------------- ------------
O>      10.10.0.0/16    10/128     10.119.254.244  00:02:22  ge1/0/2
O>      10.10.0.0/16    10/128     10.120.254.244  00:02:22  ge1/0/3
O>      10.16.2.0/24    110/128    10.119.254.244  00:02:22  ge1/0/2
O>      10.16.2.64/26   110/128    10.119.254.244  00:02:22  ge1/0/2
O>      10.16.2.64/26   110/130    10.119.254.244  00:02:22  ge1/0/3
O>      10.16.2.128/26 110/128     10.119.254.244  00:02:22  ge1/0/2
R       10.16.2.128/26 120/3       10.119.254.244  00:02:22  ge1/0/2
O>      10.16.208.0/24 110/128     10.120.254.244  00:02:22  ge1/0/2
O>      10.16.223.0/24 110/128     10.119.254.244  00:02:22  ge1/0/2
O>      10.16.236.0/24 110/129     10.119.254.240  00:02:23  ge1/0/2
R>      10.67.10.0/24   120/5      10.119.254.244  00:02:22  ge1/0/2
OE2> 10.68.132.0/24  110/5         10.119.254.6      00:00:59  ge1/0/2
O>      10.75.139.0/24  110/129    10.119.254.240 00:02:23  ge1/0/2
O>      10.84.148.0/24  110/129    10.119.254.240 00:02:23  ge1/0/2
OE2 > 10.110.0.0/24    110/128     10.119.254.6     00:01:00  ge1/0/12
C>      10.119.0.0/16   0/1        0.0.0.0                   ge1/0/2
C>      10.120.0.0/16   0/1        0.0.0.0                   ge1/0/2
```

```
O>      10.128.0.0/16   110/128     10.119.254.244 00:02:22  ge1/0/2
O>      10.129.0.0/16   110/129     10.119.254.240 00:02:02  ge1/0/2
OE2> 10.130.0.0/16    110/5        0.0.0.0             00:00:59  ge1/0/2
O>     10.140.0.0/16    110/129    10.119.254.240 00:02:23  ge1/0/2
O>      10.141.0.0/16    110/129    10.119.254.240 00:02:22  ge1/0/2
```

Example 3. In the following example, the logical AND operation is performed on the source address 10.16.0.0 and the mask 255.255.0.0, resulting in 10.16.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.16.0.0. Any destinations that fall into that range are displayed in the output:

```
Router# show ip route 10.16.0.0 255.255.0.0 longer-prefix
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled

Codes: > - best, C - connected, S - static,
       R - RIP,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP

IP Routing Table - 22 entries
Code     IP Route        Distance/  Next Hop           Last Time Outgoing
                         Metric      IP Address         Updated   Interface
------  -------------------  -----------   ---------------      ------------- ------------
O>     10.16.2.0/24      110/128    10.119.254.244  00:02:22  ge1/0/2
O>     10.16.2.64/26  110/128    10.119.254.244  00:02:22  ge1/0/2
O>     10.16.2.128/26 110/128    10.119.254.244  00:02:22  ge1/0/2
O>     10.16.208.0/24 110/128    10.120.254.244  00:02:22  ge1/0/2
O>     10.16.223.0/24 110/128    10.119.254.244  00:02:22  ge1/0/2
O>     10.16.236.0/24 110/129    10.119.254.240  00:02:23  ge1/0/2
```

Example 4. In the following example, the logical AND operation is performed on the source address 10.16.0.0 and the mask 255.255.0.0, resulting in 10.16.0.0. The destination is displayed in the output:

```
Router# show ip route 10.16.0.0 255.255.0.0 longer-prefix
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled

Codes: > - best, C - connected, S - static,
       R - RIP,
       O - OSPF intra-area, OIA - OSPF inter-area,
       OE1 - OSPF external 1, OE2 - OSPF external 2,
       B - BGP
```

```
IP Routing Table - 22 entries
Code    IP Route       Distance/  Next Hop          Last Time Outgoing
                       Metric     IP Address        Updated   Interface
------  -------------------  -----------  ---------------  ------------- ------------
O>      10.16.2.0/24    110/128   10.119.254.244  00:02:22  ge1/0/2
O>      10.16.0.0/16    10/128    10.120.254.244  00:02:22  ge1/0/3
```

47.15 show ip route summary

Use the **show ip route summary** command in User EXEC or Privileged EXEC mode to display the current contents of the IP routing table in summary format.

Syntax

show ip route summary

Parameters

N/A.

Command Mode

User EXEC

Privileged EXEC

Example

The following is sample output from the show **ip route summary** command:

```
show ip route summary
IP Routing Table Summary - 82 entries
35 connected, 25 static, 12 RIP, 10 OSPF
Number of prefixes:
/16: 10, /18: 10, /22: 15, /24: 25, /28: 2, /30: 12
```

47.16 show key chain

To display authentication key information, use the **show key chain** command in Privileged EXEC mode.

Syntax

show key chain [*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

Example

Example 1. The following is sample output from the **show key chain** command when the current time od date is defined:

```
Router# show key chain
Current Time of Date is Feb 8 2011
Accept lifetime is configured to ignore
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 od date is not defined:

```
Router# show key chain
Current Time of Date is not defined
Accept lifetime is ignored
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)
```

48 RIP Commands

48.1 clear rip statistics

The **clear rip statistics** Privileged EXEC mode command clears statistics counters of all interfaces and all peers.

Syntax

clear rip statistics

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC

User Guidelines

Example

The following example shows how to clear all counters:

```
clear rip statistics
```

48.2 default-information originate

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

Syntax

default-information originate [**on-passive** | **route-map** *map-name*]

no default-information originate

Parameters

- **on-passive**—Sends default routes only on RIP passive interfaces.
- **route-map** *map-name*—Specifies that the routing process will generate the default route if the route map is satisfied.

Default Configuration

Default route is not generated by RIP.

Command Mode

Router configuration (config-router).

User Guidelines

When no the **on-passive** or **route-map** keyword is defined then the default route with metric 1 is sent on all RIP interfaces.

When the **on-passive** keyword is defined then the default route with metric 1 is sent only on RIP passive interfaces,

When the **map-route** keyword is defined and the map route does not contain the **set metric** command then metric 1 is applied.

When the **map-route** keyword is defined and the map route does not contain the **set interface** command then the default route is not sent.

Note. The metric specified by the command overrides the metric of the default route from the RIP Routing table, if it exists.

Example

The following example shows how to originate a default route (0.0.0.0/0) with metric 3 on VLAN 100 when route 172.17.0.0/16 or more specific one is present:

```
router rip
  default-information originate route-map condition
exit
route-map condition permit 10
  match ip address 10
  set metric 3
  set interface vlan 100
exit
ip access-list 10 permit 172.17.16.0/24
```

48.3 default-metric

The **default-metric** Router RIP configuration mode command sets the default metric value when RIP advertises routes derived by other protocols (for example, 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.

Parameters ranges

metric-value—1-15.

Default Configuration

metric-value—1.

Command Mode

Router RIP configuration.

User Guidelines

Example

The following example shows how to set the default metric to 2:

```
router rip
  default-metric 2
exit
```

48.4 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 for and specifies the type of authentication. 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** CLI command.

Default Configuration

No defined key chain.

Command Mode

IP interface mode

User Guidelines

Use the **ip rip authentication key-chain** IP Interface Configuration mode command to define a key chain name. Only one key chain may be defined per an IP interface. Each the **ip rip authentication key-chain** command overrides the previous definition.

In order to have a smooth rollover of keys in a key chain, a key should be configured with a lifetime that starts several minutes before the lifetime of the previous key expires.

Example

The following example shows how to define a chain name:

```
interface ip 1.1.1.1
```

```
  ip rip authentication key-chain alpha
exit
```

48.5 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 command. If a key chain is not defined for the IP interface or there is not a valid key then 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 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 mode:

```
interface ip 1.1.1.1
  ip rip authentication mode md5
exit
```

48.6 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 up to 8 characters in length.

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 originates 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 an IP interface. Each the **ip rip authentication-key** command overrides the previous definition.

Example

The following example shows how to define a password:

```
interface ip 1.1.1.1
  ip rip authentication mode text
  ip rip authentication-key alph$$12
exit
```

48.7 ip rip default-information originate

The **ip rip default-information originate** IP Interface generates a metric for a default route in RIP. The **no** format of the command disables the feature.

Syntax

ip rip default-information originate [**passive**] {**disable** | *metric*}

no ip rip default-information originate

Parameters

metric—Default route metric value.

Parameters Ranges

- **passive**—Sends the default route if the RIP interface is passive. If the keyword is not defined and the interface is passive the default route is not sent.
- **disable**—Do not send the default route.
- **metric**—1-15.

Default Configuration

The RIP behavior is specified by the **default-information originate** command.

Command Mode

IP interface mode

User Guidelines

Use the command to override the RIP behavior specified by the **default-information originate** command on a given IP interface.

Example

The following example shows how to enable sending of default route with metric 3:

```
interface ip 1.1.1.1
  ip rip default-information originate 3
exit
```

48.8 ip rip distribute-list in

The **ip rip distribute-list in** IP configuration mode command enables filtering of routes in incoming RIP Update messages. The **no** format of the command disables the filtering.

Syntax

ip rip distribute-list {**access** *access-list-name* | **prefix** *prefix-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 routes in incoming RIP Update messages are to be accepted and which are to be suppressed.
- **prefix-list-name**—Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching the network prefix to the prefixes in the list.

Default Configuration

No filtering

Command Mode

IP interface mode

User Guidelines

Each network from a received RIP Update message is evaluated by the access list and it is accepted only if it is permitted by the list. About details see the **ip access-list (IP standard)** and **ip prefix-list** commands.

Example

The following example shows how to define input filtering:

```
interface ip 1.1.1.1
  ip rip distribute-list 5 in
exit
```

48.9 ip rip distribute-list out

The **ip rip distribute-list out** IP configuration mode command enables filtering of routes in outgoing RIP Update messages. The **no** format of the command disables the filtering.

Syntax

ip ip rip distribute-list {**access** *access-list-name* | **prefix** *prefix-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 routes in outgoing RIP Update messages are to be sent and which are to be suppressed.
- **prefix-list-name**—Name of a prefix list. The list defines which networks are to be advertised from the Routing Table and which are to be suppressed, based upon matching the network prefix to the prefixes in the list.

Default Configuration

No filtering

Command Mode

IP interface mode

User Guidelines

Each network from the IP Forwarding table is evaluated by the list and it is included in the RIP Update message only if it is permitted by the list. About details see the **ip access-list (IP standard)** and **ip prefix-list** commands.

Example

The following example shows how to define outgoing filtering:

```
Console(config)# interface ip 1.1.1.1
Console(config-ip)# ip rip distribute-list 5 out
```

48.10 ip rip offset

The **ip rip offset** IP configuration mode command defines a metric added 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.

Parameters ranges

offset—1-15.

Default Configuration

offset—1.

Command Mode

IP interface mode

User Guidelines

Example

The following example shows how to set offset to 2:

```
interface ip 1.1.1.1
  ip rip offset 2
exit
```

48.11 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 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

User Guidelines

Use the **ip rip passive-interface** command to stop of RIP messages sending on the giving IP interface. To stop of of RIP messages sending on all interfaces, use the **passive-interface** command.

Note. The **no ip rip passive-interface** command does not override the **passive-interface** command.

Example

The following example shows how to stop of RIP messages sending:

```
interface ip 1.1.1.1
  ip rip passive-interface
exit
```

48.12 ip rip shutdown

The **ip rip shutdown** IP Interface configuration mode command changes the RIP interface state from **enabled** to **disabled**. 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** CLI command may be applied only to RIP interfaces created by the **network** CLI 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:

```
interface ip 1.1.1.1
  ip rip shutdown
exit
```

48.13 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* [**shutdown**]

no network *ip-address*

Parameters

- **ip-address**—An IP address of a switch IP interface.
- **shutdown**—RIP is enabled on the interface in the shutdown state.

Default Configuration

Does not exist.

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 **network** CLI command with the **shutdown** keyword to create RIP on an interface if you are going to change the default values of RIP configuration and the use the **no ip rip shutdown** CLI command.

Use the **no network** CLI command to remove RIP on an IP interface and remove its interface configuration.

Example

Example 1.The following example shows how to enable RIP on IP interface 1.1.1.1 with the default interface configuration:

```
router rip
 network 1.1.1.1
exit
```

Example 2. The following example enables RIP on 1.1.1.1 in the shutdown state, configures metric and starts RIP:

```
router rip
 network 1.1.1.1 shutdown
exit
interface ip 1.1.1.1
  ip rip offset 2
  no ip rip shutdown
exit
```

48.14 passive-interface (RIP)

To disable sending routing updates on all RIP IP interfaces, use the **passive-interface** command in router configuration mode. To re-enable the sending of RIP routing updates, use the **no** form of this command.

Syntax

passive-interface

no passive-interface

Parameters

Default Configuration

Routing updates are sent on all OSPF IP interfaces.

Command Mode

Router configuration (config-router)

User Guidelines

After using of the **passive-interface** command you can then configure individual interfaces where adjacencies are desired using the **no ip rip passive-interface** command.

Example

The following example sets all IP interfaces as passive and then except the IP interface 1.1.1.1:

```
router rip
  passive-interface
  network 1.1.1.1
  network 2.2.2.2
  network 3.3.3.3
exit
interface ip 1.1.1.1
 no ip rip passive-interface
exit
```

48.15 redistribute (RIP)

To redistribute routes from one routing domain into a RIP routing domain, use the **redistribute** command in the Router RIP configuration mode. To disable redistribution, use the **no** form of this command.

Syntax

redistribute *protocol* [*process-id*] [**metric** {*metric-value* | **transparent**}] [**match** {**internal** | **external 1** | **external 2**}] [**route-map** *map-tag*]

no redistribute *protocol* [*process-id*] [**metric** {*metric-value* | **transparent**}] [**match** {**internal** | **external 1** | **external 2**}] [**route-map** *map-tag*]

Parameters

- **protocol**—Source protocol from which routes are being redistributed. It can be one of the following keywords: **connected**, **static, ospf** or **bgp**.
- **process-id**—The *process-id* argument is used only together with the **ospf** keyword and specifies the appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. If it is omitted then a value of 1 is assumed.
- **metric transparent**—Causes RIP to use the source protocol metric for redistributed routes as the RIP metric. Only routes with metric less than 16 are redistributed.
- **metric** *metric-value*—Specifies the metric assigned to the redistributed routes. The value supersedes the metric value specified using the **default-metric** command.
- If the metric value is set by the route map (by the **set metric** command) then the value will supersede the metric value specified by the *metric-value* argument.
- If the **metric** keyword is not defined and the **route-map** keyword is not defined or the route map does not set a metric value then the metric is specified by the **default-metric** CLI command is

assigned to the redistributed routes. If metric value set by the route map is equal or bigger than 16 the route is not redistributed.

- **match** {**internal** | **external 1** | **external 2**}—The **match** keyword is used only together with the **ospf** keyword and specifies the criteria by which OSPF routes are redistributed into RIP. It can be one of the following:
  - **internal**—Routes that are internal to a specific autonomous system.
  - **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route.
  - **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.

By default the **internal** and **external 1** routes are redistributed.

Note. A few the **redistribute** commands with different values of the **match** keyword may be defined.

- **route-map**—Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
- **map-tag**—Identifier of a configured route map.

Default Configuration

Route redistribution is disabled

Command Mode

Router RIP configuration.

User Guidelines

Routes distributed to the source protocol are never redistributed by it

The **connected** keyword is used to redistribute to RIP routes that correspond to defined IP interfaces on which RIP is not enabled. By default, the RIP Routing Table includes only routes that correspond only to IP interfaces on which it is enabled.

The **static** keyword is used to redistribute to RIP static routes. By default, static routes are not redistributed to RIP.

The **bgp** keyword is used to redistribute from BGP to RIP routes learned by eBGP. Routes learned by iBGP are redistributed only if it was configured by the **bgp redistribue-internal** command.

Changing or disabling any keyword will not affect the state of other keywords.

Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting.

Example

Example 1.The following example enables redistribution of static routes by RIP with transparent metric:

```
router 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:

```
router rip
  redistribute static metric transparent
  no redistribute static metric transparent
exit
```

Example 3. The following example enables redistribution of static routes by RIP with default metric and then changes the metric to transparent:

```
router rip
  redistribute static
  redistribute static metric transparent
exit
```

Example 4. The following example enables redistribution of static routes by RIP with transparent metric. The second redisatribute command does not affect:

```
router rip
  redistribute static metric transparent
  redistribute static
exit
```

Example 5. The following example disables redistribution of static routes by RIP:

```
router rip
  no redistribute static
exit
```

Example 6. The following example shows how internal and extenal 1 OSPF routes are redistributed into a RIP domain:

```
router rip
  redistribute ospf 1
exit
```

Example 7. The following example shows how internal and extenal 1 OSPF routes are redistributed into a RIP domain with metric 1 and exteranal 2 OSPF routers with metric 4. The first **redistribute** command does not include the **match** keyword because it is a default value:

```
router rip
  redistribute ospf 1 metric 1
  redistribute ospf 1 match external 2 metric 4
```

```
exit
```

Example 8. The following example configures BGP routes to be redistributed into RIP. The metric is specified as 5:

```
router rip
  redistribute bgp 120 metric 5
exit
```

Example 9. The following example removes the metric 5 option causing using of a metric defined by the default-metric CLI command:

```
router rip
  no redistribute static metric 1000
exit
```

Example 10. The following example removes the route-map m103:

```
router rip
  no redistribute ospf route-map m103
exit
```

48.16 router rip

The **router rip** Global Configuration mode command specifies the Router RIP mode and enables it if it was disabled. 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
- enabled
- shutdown

If a value of the RIP global state is **disabled** (default value), RIP is not operational and cannot be configured. When the state is set, the RIP configuration is removed. The state may be set by the **no router rip** CLI command from any RIP global state.

If a value of the RIP global state is **shutdown,** RIP is not operational, but can be configured. When the state is set the RIP configuration is not changed. The state may be set by the **shutdown** CLI command from the **enabled** RIP global state.

If the value of the RIP global state is **enabled**, RIP is operational, and can be configured. The state may be 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.

Example

The following example shows how to enable RIP globally:

```
router rip
```

48.17 show ip rip database

The **show ip rip database** Privileged EXEC mode command displays information about 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.

Command Mode

Privileged EXEC mode

Default Configuration

User Guidelines

Example

Example 1. The following example shows the full RIP database information about all RIP interfaces is displayed:

```
Console#show ip rip database
RIP is enabled
RIP Administrative state is UP
Default metric value is 1
Redistributing is enabled from
  Connected:
   Metric is default-metric
   no route-map
  Static:
    Metric is transparent
    no route-map
  OSPF 109:
    internal:
      metric value is 2
      no route-map name
    external 1
      metric value is 4
      no route-map
    external 2
      metric is value 6
      route-map name is route-map-ospf-exter2
      with subnets

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
IN Filtering Type is Prefix List
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
Default Originate Metric 3, on passive too
No Authentication
No IN Filtering
No OUT Filtering

IP Interface: 4.4.4.4
Administrative State is shutdown
IP Interface Offset is 1
No Authentication
No IN Filtering
No OUT Filtering
```

Example 2. The following example shows the full RIP database information about a given IP address is displayed:

```
Console#show ip rip database 1.1.1.1
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: on passive only
Default metric value is 1
Redistributing is enabled from
  Connected
   Metric is default-metric
   no route-map
  Static:
    Metric is transparent
    no route-map
  OSPF:
    from metric type:
      metric value is 2
      no route-map name
    exteranl 1
      metric value is 4
      no route-map
    exteranl 2
      metric is value 6
      route-map name is route-map-ospf-exter2
      with subnets

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 breif RIP database information about all RIP interfaces is displayed:

```
Console#show ip rip database brief
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: route-map is condition
Default metric value is 1
Redistributing is enabled from
  Connected
    Metric is default-metric
    no route-map
  Static
    Metric is transparent
    no route-map
  OSPF 1
    from metric type:
      metric value is 2
      no route-map name
     exteranl 1
       metric value is 4
       no route-map
     exteranl 2
       metric is value 6
       route-map name is route-map-ospf-exter2
       with subnets

IP Interface    Admin    Offset  Passive   Default Auth.  IN Filt. OUT Filt.
                State            Interface Metric  Type   Type     Type
--------------- -------- ------- --------  ------- -----  -------  ---------
100.100.100.100 enabled    10      No         12   Text   Access   Access
2.2.2.2         enabled     2      No              MD5    Prefix   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:

```
Console#show ip rip database
RIP is disabled
```

48.18 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

Command Mode

Privileged EXEC mode

Default Configuration

User Guidelines

Example

```
Console>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          -              -
```

48.19 show ip rip statistics

The **show ip rip statistics** Privileged EXEC mode command displays RIP Statistics.

Syntax

show ip rip statistics

Parameters

N/A

Command Mode

Privileged EXEC mode

Default Configuration

User Guidelines

Example

```
Console#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
```

48.20 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 stop RIP globally without removing its configuration

Example

The following example shows how to shutdown RIP globally:

```
router rip
  shutdown
exit
```

49 IPv6 Router Commands

49.1 clear ipv6 neighbors

Use the **clear ipv6 neighbors** command in privileged EXEC mode to delete all entries in the IPv6 neighbor discovery cache, except static entries.

Syntax

clear ipv6 neighbors

Parameters

N/A

Command Mode

Privileged EXEC

User Guidelines

Example

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
clear ipv6 neighbors
```

49.2 clear ipv6 prefix-list

Use the **clear ipv6 prefix-list** command in privileged EXEC mode to reset the hit count of the IPv6 prefix list entries.

Syntax

clear ipv6 prefix-list [*prefix-list-name* [*ipv6-prefix*/*prefix-length*]]

Parameters

- **prefix-list-name**—The name of the prefix list from which the hit count is to be cleared.
- **ipv6-prefix**—The IPv6 network from which the hit count is to be cleared. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—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 value.

Default Configuration

The hit count is automatically cleared for all IPv6 prefix lists.

Command Mode

Privileged EXEC

User Guidelines

The **clear ipv6 prefix-list** command is similar to the **clear ip prefix-list** command, except that it is IPv6-specific.

The hit count is a value indicating the number of matches to a specific prefix list entry.

Example

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35:

```
clear ipv6 prefix-list first_list 2001:0DB8::/35
```

49.3 ipv6 address

Use the **ipv6 address** command in Interface Configuration mode to configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface. To remove the address from the interface, use the **no** form of this command.

Syntax

ipv6 address *ipv6-address*/*prefix-length*

no ipv6 address [*ipv6-address*/*prefix-length*]

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **prefix-length**—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 value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration

User Guidelines

Using the **no IPv6 address** command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

The following example defines the IPv6 global address 2001:DB8:2222:7272::72 on vlan 100:

```
interface vlan 100
  ipv6 address 2001:DB8:2222:7272::72/64
exit
```

49.4 ipv6 address anycast

Use the **ipv6 address anycast** command in Interface Configuration mode to configure an IPv6 Anycast address and enable IPv6 processing on an interface.

To remove the address from the interface, use the **no** form of this command.

Syntax

ipv6 address *ipv6-prefix*/*prefix-length* **anycast**

no ipv6 address [*ipv6-prefix*/*prefix-length* **anycast**]

Parameters

- **pv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **prefix-length**—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 value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration

User Guidelines

An Anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes. A packet sent to an Anycast address is delivered to the closest interface—as defined by the routing protocols in use—identified by the Anycast address. Anycast addresses are syntactically indistinguishable from Unicast addresses because Anycast addresses are allocated from the Unicast address space. Nodes to which the Anycast address is assigned must be explicitly configured to recognize that the address is an Anycast address.

Anycast addresses can be used only by a router, not a host, and Anycast addresses must not be used as the source address of an IPv6 packet.

The subnet router Anycast address has a prefix concatenated by a series of zeros (the interface ID). The subnet router Anycast address can be used to reach a router on the link that is identified by the prefix in the subnet router Anycast address.

Using the **no IPv6 address** command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

The following example enables IPv6 processing on the interface, assigns the prefix 2001:0DB8:1:1::/64 to the interface, and configures the IPv6 Anycast address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE:

```
interface vlan 1
  ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
exit
```

49.5 ipv6 address autoconfig

Use the **ipv6 address autoconfig** command in Interface Configuration mode to enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.

To remove the address from the interface, use the **no** form of this command.

Syntax

ipv6 address autoconfig

no ipv6 address autoconfig

Parameters

N/A.

Default Configuration

Stateless Auto configuration is disabled.

Command Mode

Interface Configuration mode.

User Guidelines

This command enables IPv6 on an interface (if it was disabled) and causes the switch to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the eui-64 based addresses to the interface.

Stateless auto configuration is applied only when IPv6 Forwarding is disabled.

When IPv6 forwarding is changed from disabled to enabled, and stateless auto configuration is enabled the switch stops stateless auto configuration and removes all stateless auto configured ipv6 addresses from all interfaces.

When IPv6 forwarding is changed from enabled to disabled and stateless auto configuration is enabled the switch resumes stateless auto configuration.

Using the **no ipv6 address autoconfig** command to disable stateless auto configuration and to remove all stateless auto configured IPv6 addresses from an interface.

Example

The following example assigns the IPv6 address automatically:

```
interface vlan 100
  ipv6 address autoconfig
exit
```

49.6 ipv6 address eui-64

Use the **ipv6 address eui-64** command in Interface Configuration mode to configure an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address.

To remove the address from the interface, use the **no** form of this command.

Syntax

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix*/*prefix-length* **eui-64**]

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **prefix-length**—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 value.

Default Configuration

No IP address is defined for the interface.

Command Mode

Interface Configuration

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.

If the switch detects another host using one of its IPv6 addresses, it adds the IPv6 address and displays an error message on the console.

Using the **no IPv6 address** command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually-configured addresses.

Example

The following example enables IPv6 processing on VLAN 1, configures IPv6 global address 2001:0DB8:0:1::/64 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
interface vlan 1
  ipv6 address 2001:0DB8:0:1::/64 eui-64
exit
```

49.7 ipv6 address link-local

Use the **ipv6 address link-local** command in Interface Configuration mode to configure an IPv6 link local address for an interface and enable IPv6 processing on the interface.

To remove the manually configured link local address from the interface, use the **no** form of this command.

Syntax

ipv6 address *ipv6-prefix* **link-local**

no ipv6 address [**link-local**]

Parameters

- **ipv6-address**—Specifies the IPv6 network assigned to the interface. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.

Default Configuration

The default Link-local address is defined.

Command Mode

Interface Configuration

User Guidelines

The switch automatically generates a link local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link local address to be used by an interface, use the **ipv6 address link-local** command.

Using the **no IPv6 address** command without arguments removes all manually-configured IPv6 addresses from an interface, including link local manually configured addresses.

Example

The following example enables IPv6 processing on VLAN 1 and configures FE80::260:3EFF:FE11:6770 as the link local address for VLAN 1:

```
interface vlan 1
  ipv6 address FE80::260:3EFF:FE11:6770 link-local
exit
```

49.8 ipv6 default-gateway

Use the **ipv6 default-gateway** Global Configuration mode command to define an IPv6 default gateway.

To remove the default gateway, use the **no** form of this command.

Syntax

ipv6 default-gateway *ipv6-address* | *interface-id*

no ipv6 default-gateway *ipv6-address* | *interface-id*

Parameters

- **ipv6-address**—Specifies the IPv6 address of the next hop that can be used to reach a network.
- **interface-id**—Specifies the Interface Identifier of the outgoing interface that can be used to reach a network.

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

User Guidelines

The command is an alias of the **ipv6 route** command with the predefined (default) route:

ipv6 route ::/0 *ipv6-address* | *interface-id*

See the definition of the **ipv6 route** command for details.

Example The following example configures a default gateway:

```
console(config)# ipv6 default-gateway fe80::abcd%vlan1
```

49.9 ipv6 distance

Use the **ipv6 distance** command in Global Configuration mode to define the administrative distance for routes that are inserted into the routing table.

To return the administrative distance to its default distance definition, use the **no** form of this command.

Syntax

ipv6 distance {**static** | **igmp**} *distance*

no ipv6 distance {**static** | **igmp**}

ipv6 distance ospf {**inter-as** | **intra-as**} *distance*

no ipv6 distance ospf {**inter-as** | **intra-as**}

ipv6 distance bgp {**external** | **internal** | **local**} *distance*

no ipv6 distance bgp {**external** | **internal** | **local**}

Parameters

- **static**—Administrative distance for static routes.
- **igmp**—Administrative distance for routes learned from the ICMP Redirect messages.
- **ospf**—Administrative distance for OSPF for IPv6 routes.
- **bgp**—Administrative distance for BGP for IPv6 routes.
- **ospf inter-as** —Administrative distance for OSPF routes from one Autonomous System to another Autonomous System (LSAs type 5 and type 7 routes, external 2 metric).
- **ospf intra-as**—Administrative distance for OSPF routes within an Autonomous System (Internal and External 1 metric.
- **bgp external**—Administrative distance for BGP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.
- **bgp internal**—Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
- **bgp local**—Administrative distance for BGP local routes. Local routes are those networks listed with a network router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
- *distance*—Administrative distance. An integer from 1 to 255. A value of 0 is reserved for **connected** routes that cannot be changed.

Default Configuration

connected—0

static—1

igmp—2

ospf intra-as—30

ospf inter-as—110

bgp external—20

bgp internal—200

bgp local—200

Command Mode

Global Configuration mode

User Guidelines

An administrative distance is a rating of the trust worthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Example

In the following example, distance 20 is set for OSPF intra-as routes and distance 40 is set for BGP local routes:

```
ipv6 distance ospf intra-as 20
ipv6 distance bgp local 40
```

49.10 ipv6 enable

Use the **ipv6 enable** command in Interface Configuration mode to enable IPv6 processing on an interface.

To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

Syntax

ipv6 enable

no ipv6 enable

Parameters

N/A.

Default Configuration

IPv6 addressing is disabled.

Command Mode

Interface Configuration

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 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Example

The following example enables VLAN 1 for the IPv6 addressing mode.

```
interface vlan 1
  ipv6 enable
exit
```

49.11 ipv6 hop-limit

Use the **ipv6 hop-limit** command in Global Configuration mode to configure the maximum number of hops used in all IPv6 packets that are originated by the router.

To return the hop limit to its default value, use the **no** form of this command.

Syntax

ipv6 hop-limit *value*

no ipv6 hop-limit

Parameters

value—Maximum number of hops. The acceptable range is from 1 to 255.

Default Configuration

The default is 64 hops.

Command Mode

Global Configuration

Example

The following example configures a maximum number of 15 hops for all IPv6 packets that are originated from the router:

```
ipv6 hop-limit 15
```

49.12 ipv6 icmp error-interval

Use the **ipv6 icmp error-interval** command in Global Configuration mode to configure the interval and bucket size for IPv6 ICMP error messages. To return the interval to its default setting, use the **no** form of this command.

Syntax

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

Parameters

- *milliseconds*—Time interval between tokens being placed in the bucket. Each token represents a single ICMP error message. The acceptable range is from 0 to 2147483647. A value of 0 disables ICMP rate limiting.
- *bucketsize*—Maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200.

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

Use this command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens arriving in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Average Packets Per Second = (1000/ *milliseconds*) * *bucketsize*.

To disable ICMP rate limiting, set the *milliseconds* argument to zero.

Example

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
ipv6 icmp error-interval 50 20
```

49.13 ipv6 link-local default zone

Use the **Ipv6 link-local default zone** 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.

Default

By default, **link local default zone** is disabled.

Command Mode

Global Configuration mode

Example

The following example defines VLAN 1 as a default zone:

```
ipv6 link-local default zone vlan1
```

49.14 ipv6 mld version

Use the **ipv6 mld version** Interface Configuration mode command to specify the version of the MLD.

To return to the default version, use the **no** form of this command.

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

Example

The following example defines MLDv2 on VLAN 1:

```
console(config)# interface vlan 1
console(config-if)# ipv6 mld version 2
```

49.15 ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** in Interface Configuration mode to configure the advertisement interval option in router advertisements (RAs).

To reset the interval to the default value, use the **no** form of this command.

Syntax

ipv6 nd advertisement-interval

no ipv6 nd advertisement-interval

Parameters

N/A.

Default Configuration

Advertisement interval option is not sent.

Command Mode

Interface Configuration

User Guidelines

Use the **ipv6 nd advertisement-interval** command to indicate to a visiting mobile node the interval at which that node may expect to receive RAs. The node may use this information in its movement detection algorithm.

Example

The following example enables the advertisement interval option to be sent in RAs:

```
interface vlan 1
  ipv6 nd advertisement-interval
exit
```

49.16 ipv6 nd dad attempts

Use the **ipv6 nd dad attempts** command in Interface Configuration mode to configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the Unicast IPv6 addresses of the interface.

To return the number of messages to the default value, use the **no** form of this command.

Syntax

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts

Parameters

value—The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions.

Default Configuration

1

Command Mode

Interface Configuration

User Guidelines

Duplicate address detection verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of Unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 4862, IPv6 Stateless Address Autoconfiguration) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface, while duplicate address detection is performed on a tentative Unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 4861, Neighbor Discovery for IPv6), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the **ipv6 nd ns-interval** command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the Unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up.

An interface returning to administratively up, restarts duplicate address detection for all of the Unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address 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 SYSLOG message is issued.

If the duplicate address is a global address of the interface, the address is not used and an error SYSLOG message is issued.

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Note. The configuration is saved and will impacted when the interface type is changed on another type on which DAD is supported (for example, to the IPv6 manual tunnel).

Example

The following example configures five consecutive neighbor solicitation messages to be sent on VLAN 1 while duplicate address detection is being performed on the tentative Unicast IPv6 address of the interface. The example also disables duplicate address detection processing on VLAN 2.

```
interface vlan 1
  ipv6 nd dad attempts 5
exit
interface vlan 2
```

```
  ipv6 nd dad attempts 0
exit
```

49.17 ipv6 nd hop-limit

Use the **ipv6 nd hop-limit** command in Global Configuration mode to configure the maximum number of hops used in router advertisements.

To return the hop limit to its default value, use the **no** form of this command.

Syntax

ipv6 nd hop-limit *value*

no ipv6 nd hop-limit

Parameters

value—Maximum number of hops. The acceptable range is from 1 to 255.

Default Configuration

The default value is defined by the **ipv6 hop-limit** command, or is set to 64 hops, if the command was not configured.

Command Mode

Interface Configuration

User Guidelines

Use this command if you want to change the default value. The default value is defined by the **ipv6 hop-limit** command.

Example

The following example configures a maximum number of 15 hops for router advertisements on VLAN 2:

```
interface vlan 2
  ipv6 nd hop-limit 15
exit
```

49.18 ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command in Interface Configuration mode to set the “managed address configuration flag” in IPv6 router advertisements.

To clear the flag from IPv6 router advertisements, use the **no** form of this command.

Syntax

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameters

N/A.

Default Configuration

The “managed address configuration flag” flag is not set in IPv6 router advertisements.

Command Mode

Interface Configuration

User Guidelines

Setting the Managed Address Configuration flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If this flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses, and if it is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Example

The following example configures the Managed Address Configuration flag in IPv6 router advertisements on VLAN 1:

```
interface vlan 1
  ipv6 nd managed-config-flag
exit
```

49.19 ipv6 nd ns-interval

Use the i**pv6 nd ns-interval** command in Interface Configuration mode to configure the interval between IPv6 neighbor solicitation retransmissions on an interface.

To restore the default interval, use the **no** form of this command.

Syntax

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameters

milliseconds—Interval between IPv6 neighbor solicit transmissions. The acceptable range is from 1000 to 3600000 milliseconds.

Default Configuration

0 seconds (unspecified) is advertised in router advertisements and the value 1000 milliseconds is used for the neighbor discovery activity of the router itself.

Command Mode

Interface Configuration

User Guidelines

This value will be included in all IPv6 router advertisements sent out this interface. Very short intervals are not recommended in normal IPv6 operation. When a non-default value is configured, the configured time is both advertised and used by the router itself.

Example

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for VLAN 1:

```
interface vlan 1
  ipv6 nd ns-interval 9000
exit
```

49.20 ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command in Interface Configuration mode to set the Other Stateful configuration flag in IPv6 router advertisements.

To clear the flag from IPv6 router advertisements, use the **no** form of this command.

Syntax

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameters

N/A.

Default Configuration

The Other Stateful configuration flag is not set in IPv6 router advertisements.

Command Mode

Interface Configuration

User Guidelines

The setting of the Other Stateful configuration flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.

Note. If the Managed Address Configuration flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the Other Stateful configuration flag.

Example

The following example configures the Other Stateful configuration flag in IPv6 router advertisements on VLAN 1:

```
interface vlan 1
  ipv6 nd other-config-flag
```

```
exit
```

49.21 ipv6 nd prefix

Use the **ipv6 nd prefix** command in Interface Configuration mode to configure which IPv6 prefixes are included in IPv6 Neighbor Discovery (ND) router advertisements.

To remove the prefixes, use the **no** form of this command.

Syntax

ipv6 nd prefix {*ipv6-prefix***/***prefix-length* | **default**} [**no-advertise** | {[*valid-lifetime preferred-lifetime*] [**no-autoconfig**] [**off-link** | **no-onlink**]}]

no ipv6 nd prefix [*ipv6-prefix*/*prefix-length* | **default**]

Parameters

- **ipv6-prefix**—IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC4293, where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—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 value.
- **default**—Default values used for automatic advertised prefixes configured as addresses on the interface using the ipv6 address command.
- **no-advertise**—Prefix is not advertised.
- **valid-lifetime**—Remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. A value of 4,294,967,295 represents infinity. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.
- **preferred-lifetime**—Remaining length of time, in seconds, that this prefix will continue to be preferred, i.e., time until deprecation. A value of 4,294,967,295 represents infinity. The address generated from a deprecated prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The *preferred-lifetime* must not be larger than the *valid-lifetime*.
- **no-autoconfig**—Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.The prefix will be advertised with the A-bit clear.
- **off-link**—Configures the specified prefix as off-link. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured using the **ipv6 address** command), then it will be removed.
- **no-onlink**—Configures the specified prefix as not on-link. The prefix will be advertised with the L-bit clear.

Default Configuration

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2,592,000 seconds (30 days) and a preferred lifetime of 604,800 seconds (7 days).

Note that by default:

- All prefixes are inserted in the routing table as connected prefixes.
- All prefixes are advertised as on-link (for example, the L-bit is set in the advertisement)
- All prefixes are advertised as an auto-configuration prefix (for example, the A-bit is set in the advertisement)

Command Mode

Interface Configuration

User Guidelines

This command enables control over the individual parameters per prefix, including whether the prefix should be advertised.

Use the **ipv6 nd prefix** *ipv6-prefix/prefix-length* command to add the prefix to the Prefix table.

Use the **no ipv6 nd prefix** *ipv6-prefix*I*prefix-length* command to remove the prefix from the Prefix table.

Use the **no ipv6 nd prefix** command without the *ipv6-prefix*I*prefix-length* argument o remove all prefixes from the Prefix Table.

Note. The **no ipv6 nd prefix** command does not return the default values to the original default values.

The switch supports the following advertisement algorithm:

- Advertise all prefixes that are configured as addresses on the interface using the parameters defined by the **ipv6 nd prefix default** command (or the default value if the command has not been configured) except refixes that are placed in the Prefix table (changed (configured) by the **ipv6 nd prefix** command).
- Advertise all prefixes configured by the **ipv6 nd prefix** command without the **no-advertise** keyword.

Default Keyword

The **default** keyword can be used to set default values for automatic advertised prefixes configured as addresses on the interface using the **ipv6 address** command.

Note. These default values are not used as the default values in the **ipv6 nd prefix** command.

Use the **no ipv6 nd prefix default** command to return the default values to the original default values.

On-Link

When on-link is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. An on-link prefix is inserted into the routing table as a Connected prefix.

Auto-configuration

When auto-configuration is on (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 auto-configuration.

The configuration options affect the L-bit and A-bit settings associated with the prefix in the IPv6 ND Router Advertisement, and presence of the prefix in the routing table, as follows:

■ **Default**	L=1 A=1, In the Routing Table
■ **no-onlink**	L=0 A=1, In the Routing Table
■ **no-autoconfig**	L=1 A=0, In the Routing Table
■ **no-onlink no-autoconfig**	L=0 A=0, In the Routing Table
■ **off-link**	L=0 A=1, Not in the Routing Table
■ **off-link no-autoconfig**	L=0 A=0, Not in the Routing Table

Example

Example 1. The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out VLAN 1 with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds. The prefix is inserted in the Routing table:

```
interface vlan 1
  ipv6 nd prefix 2001:0DB8::/35 1000 900
exit
```

Example 2. The following example advertises the prefix with the L-bit clear:

```
interface vlan 1
  ipv6 address 2001::1/64
  ipv6 nd prefix 2001::/64 3600 3600 no-onlink
exit
```

49.22 ipv6 nd ra interval

Use the **ipv6 nd ra interval** command in Interface Configuration mode to configure the interval between IPv6 router advertisement (RA) transmissions on an interface.

To restore the default interval, use the **no** form of this command.

Syntax

ipv6 nd ra interval *maximum-secs* [*minimum-secs*]

no ipv6 nd ra interval

Parameters

- **maximum-secs**—Maximum interval between IPv6 RA transmissions in seconds. The range is from 4 to 1800.
- **minimum-secs**—Minimum interval between IPv6 RA transmissions in seconds. The range is from 3 to 1350.

Default Configuration

maximum-secs is 600 seconds.

minimum-secs is 0.33**maximum-secs,* if the value .=> 3 seconds and is 3 seconds, if the value .< 3 seconds.

Command Mode

Interface Configuration

User Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using this command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.

The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds.

Example

Example 1. The following example configures an IPv6 router advertisement interval of 201 seconds for VLAN 1:

```
interface vlan 1
  ipv6 nd ra interval 201
exit
```

Example 2. The following examples shows a maximum RA interval of 200 seconds and a minimum RA interval of 50 seconds:

```
interface vlan 1
  ipv6 nd ra interval 200 50
exit
```

49.23 ipv6 nd ra lifetime

Use the **ipv6 nd ra lifetime** command in Interface Configuration mode to configure the Router Lifetime value in IPv6 router advertisements on an interface.

To restore the default lifetime, use the **no** form of this command.

Syntax

ipv6 nd ra lifetime *seconds*

no ipv6 nd ra lifetime

Parameters

seconds—Remaining length of time, in seconds, that this router will continue to be useful as a default router (Router Lifetime value). A value of zero indicates that it is no longer useful as a default router. The acceptable range is 0 or from <Maximum RA Interval> to 9000 seconds.

Default Configuration

The default lifetime value is 3*<Maximum RA Interval> seconds.

Command Mode

Interface Configuration

User Guidelines

The Router Lifetime value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The Router Lifetime value can be set to a non-zero value to indicate that it should be considered a default router on this interface. The non-zero value for the Router Lifetime value should not be less than the router advertisement interval.

Example

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for VLAN 1:

```
interface vlan 1
  ipv6 nd ra lifetime 1801
exit
```

49.24 ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command in Interface Configuration mode to suppress IPv6 router advertisement transmissions on an interface. To re-enable the sending of IPv6 router advertisement transmissions on an interface, use the **no** form of this command.

Syntax

ipv6 nd ra suppress

no ipv6 nd ra suppress

Parameters

N/A.

Default Configuration

LAN interface - IPv6 router advertisements are automatically sent.

Point-to-Point interface - IPv6 router advertisements are suppressed.

NBMA interface - IPv6 router advertisements are suppressed.

Command Mode

Interface Configuration

User Guidelines

Use the **no ipv6 nd ra suppress** command to enable the sending of IPv6 router advertisement transmissions on a Point-to-Point interface (for example, manual tunnel).

Use the **no ipv6 nd ra suppress** command to enable the sending of IPv6 router advertisement transmissions on a NBMA interface (for example, a tunnel).

Example

Example 1. The following example suppresses IPv6 router advertisements on vlan 1:

```
interface vlan 1
  ipv6 nd ra suppress
exit
```

Example 2. The following example enables the sending of IPv6 router advertisements on tunnel 1:

```
interface tunnel 1
```

```
  no ipv6 nd ra suppress
exit
```

49.25 ipv6 nd reachable-time

Use the **ipv6 nd reachable-time** command in Interface Configuration mode to configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

To restore the default time, use the **no** form of this command.

Syntax

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameters

milliseconds—Amount of time that a remote IPv6 node is considered reachable (in milliseconds). The acceptable range is from 0 to 3600000 milliseconds.

Default Configuration

0 milliseconds (unspecified) is advertised in router advertisements and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

Command Mode

Interface Configuration

User Guidelines

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 means indicates that the configured time is unspecified by this router.

Example

The following example configures an IPv6 reachable time of 1,700,000 milliseconds for VLAN 1:

```
interface vlan 1
  ipv6 nd reachable-time 1700000
exit
```

49.26 ipv6 nd router-preference

Use the **ipv6 nd router-preference** command in Interface Configuration mode to configure a default router preference (DRP) for the router on a specific interface.

To return to the default DRP, use the **no** form of this command.

Syntax

ipv6 nd router-preference {***high*** | ***medium*** | ***low***}

no ipv6 nd router-preference

Parameters

- **high**—Preference for the router specified on an interface is high.
- **medium**—Preference for the router specified on an interface is medium.
- **low**—Preference for the router specified on an interface is low.

Default Configuration

Router advertisements (RAs) are sent with the medium preference.

Command Mode

Interface Configuration

User Guidelines

RA messages are sent with the DRP configured by the this command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when, for example, two routers on a link may provide equivalent, but not equal-cost, routing, and policy may dictate that hosts should prefer one of the routers.

Example

The following example configures a DRP of high for the router on VLAN 1:

```
interface vlan 1
  ipv6 nd router-preference high
exit
```

49.27 ipv6 neighbor

Use the **ipv6 neighbor** command in Global Configuration mode to configure a static entry in the IPv6 neighbor discovery cache. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the **no** form of this command.

Syntax

i**pv6 neighbor** *ipv6-address interface-id mac-address*

no ipv6 neighbor [[*ipv6-address*] *interface-id*]

Parameters

- **ipv6-address**—Specified IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **interface-id**—Specified interface identifier.
- **mac-address**—Interface MAC address.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration

User Guidelines

This command is similar to the **arp** (global) command.

Use the i**pv6 neighbor** command to add a static entry in the IPv6 neighbor discovery cache.

If the specified IPv6 address is a global IPv6 address it must belong to one of static on-link prefixes defined in the interface. When a static on-link prefix is deleted all static entries in the IPv6 neighbor discovery cache corresponding the prefix is deleted to.

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.

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Use the **no ipv6 neighbor** *ipv6-address interface-id* command to remove the one given static entry on the given interface. The command does not remove the entry from the cache, if it is a dynamic entry, learned from the IPv6 neighbor discovery process.

Use the **no ipv6 neighbor** *interface-id* command to delete the all static entries on the given interface.

Use the **no ipv6 neighbor** command to remove the all static entries on all interfaces.

Use the **show ipv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- NCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.

Note. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries.

Example

Example 1. The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
ipv6 neighbor 2001:0DB8::45A vlan1 0002.7D1A.9472
```

Example 2. The following example deletes the static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on VLAN 1:

```
no ipv6 neighbor 2001:0DB8::45A vlan1
```

Example 3. The following example deletes all static entries in the IPv6 neighbor discovery cache on VLAN 1:

```
no ipv6 neighbor vlan1
```

Example 4. The following example deletes all static entries in the IPv6 neighbor discovery cache on all interfaces:

```
no ipv6 neighbor
```

49.28 ipv6 prefix-list

Use the **ipv6 prefix-list** command in Global Configuration mode to create an entry in an IPv6 prefix list. To delete the entry, use the **no** form of this command.

Syntax

ipv6 prefix-list *list-name* [**seq** *number*] {{**deny**|**permit**} *ipv6-prefix*/*prefix-length* [**ge** *ge-length*] [**le** *le-length*]} | **description** *text*

no ipv6 prefix-list *list-name* [**seq** *number*]

Parameters

- **list-name**—Name of the prefix list. The name may contain up to 32 characters.
- **seq** *seq-number*—Sequence number of the prefix list entry being configured. It is an integer value from 1 to 4294967294.
- **deny**—Denies networks that matches the condition.
- **permit**—Permits networks that matches the condition.
- **ipv6-prefix**—IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal—using 16-bit values between colons.
- **/prefix-length**—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 value from 0 to 128. The zero *prefix-length* may be used only with the zero *ipv6-prefix* (::).
- **description** *text*—Comment entry with text that can be up to 80 characters in length.
- **ge** *ge-value*—Specifies a prefix length greater than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the lowest value of a range of the length (the “from” portion of the length range).
- **le le-value**—Specifies a prefix length less than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the highest value of a range of the length (the “to” portion of the length range).

Default Configuration

No prefix list is created.

Command Mode

Global Configuration

User Guidelines

This command is similar to the **ip prefix-list** command, except that it is IPv6-specific.

This command without the **seq** keyword adds the new entry after the last entry of the prefix list with the sequence number equals to the last number plus 5. For example, if the last configured sequence number is 43, the new entry will have the sequence number of 48. If the list is empty, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.

This command with the **seq** keyword puts the new entry into the place specified by the parameter, if an entry with the number exists it is replaced by the new one.

The **no ipv6 prefix-list** command without the **seq** keyword removes the prefix list.

The **no ipv6 prefix-list** command with the **seq** keyword removes the specified entry.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you might want to put the most common permits or denies near the top of the list, using the seq-number argument.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual *ipv6-prefix*/*prefix-length* argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

- The candidate prefix must match the specified prefix list and prefix length entry
- The value of the optional le keyword specifies the range of allowed prefix lengths from the prefix-length argument up to, and including, the value of the le keyword
- The value of the optional ge keyword specifies the range of allowed prefix lengths from the value of the ge keyword up to, and including, 128.

Note that the first condition must match before the other conditions take effect.

An exact match is assumed when the **ge** or **le** keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The *prefix-length* value must be less than the **ge** value. The ge value must be less than, or equal to, the **le** value. The **le** value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have any permit and deny condition statements, has an implicit **deny any any** statement as its last match condition.

Formal Specification

Checked prefix is **cP** and checked prefix length is **cL**.

Function **PrefixIsEqual**(P1, P2, L) compares the first L bits of two addresses P1 and P2 and returns TRUE if they are equal.

Case 1. A prefix-list entry is:

- **P** - prefix address
- **L** - prefix length
- **ge** - is not defined
- **le** - is not defined

The prefix cP/cL matches the prefix-list entry if **PrefixIsEqual**(cP,P,L) && **cL** == **L**

Case 2. An prefix-list entry is:

- **P** - prefix address
- **L** - prefix length
- **ge** - is defined
- **le** - is not defined

The prefix cP/cL matches the prefix-list entry if **PrefixIsEqual**(cP,P,L) && **cL** >= **ge**

Case 3. An prefix-list entry is:

- **P** - prefix address
- **L** - prefix length
- **ge** - is not defined
- **le** - is defined

The prefix cP/cL matches to the prefix-list entry if **PrefixIsEqual**(cP,P,L) && **cL** <= **le**

Case 4. An prefix-list entry is:

- **P** - prefix address
- **L** - prefix length
- **ge** - is defined
- **le** - is defined

The prefix cP/cL matches the prefix-list entry if **PrefixIsEqual**(cP,P,L) && **ge** <= **cL** <= **le**

Example

Example 1. The following example denies all routes with a prefix of ::/0:

```
ipv6 prefix-list abc deny ::/0
```

Example 2. The following example permits the prefix 2002::/16:

```
ipv6 prefix-list abc permit 2002::/16
```

Example 3. The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64:

```
ipv6 prefix-list abc permit 5F00::/48 le 64
```

Example 4. The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64:

```
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

Example 5. The following example permits mask lengths from 32 to 64 bits in all address space:

```
ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

Example 6. The following example denies mask lengths greater than 32 bits in all address space:

```
ipv6 prefix-list abc deny ::/0 ge 32
```

Example 7. The following example denies all routes with a prefix of 2002::/128:

```
ipv6 prefix-list abc deny 2002::/128
```

Example 8. The following example permits all routes with a prefix of ::/0:

```
ipv6 prefix-list abc permit ::/0
```

49.29 ipv6 redirect

Use the **ipv6 redirects** command in Interface Configuration mode to enable the sending of ICMP IPv6 redirect messages to re-send a packet through the same interface on which the packet was received.

To disable the sending of redirect messages, use the **no** form of this command.

Syntax

ipv6 redirect

no ipv6 redirect

Parameters

N/A.

Default Configuration

The sending of ICMP IPv6 redirect messages is enabled.

Command Mode

Interface Configuration.

User Guidelines

The rate at which the router generates all IPv6 ICMP error messages can be limited by using this command.

Example

The following example disables the sending of ICMP IPv6 redirect messages on VLAN 100 and re-enables the messages on VLAN 2:

```
interface vlan 100
  no ipv6 redirect
exit
interface vlan 2
  ipv6 redirect
exit
```

49.30 ipv6 route

Use the **ipv6 route** command in Global Configuration mode to establish static IPv6 routes.

To remove a previously configured static route, use the **no** form of this command.

Syntax

ipv6 route *ipv6-prefix*/*prefix-length* {*next--ipv6-address* | *interface-id*} [*metric*]

no ipv6 route *ipv6-prefix*/*prefix-length* {*next--ipv6-address* | *interface-id*}

Parameters

- **ipv6-prefix**—IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured.
- **/prefix-length**—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 value.
- **next-ipv6-address**—IPv6 address of the next hop that can be used to reach the specified network.
  - If the *next--ipv6-address* argument is a link local address it must be defined in the zone format: IPv6 Zone Format> ::= *IPv6-Link-Local-Address***%***Interface-ID*
  - The *interface-id* argument must be coded without spaces.
- **interface-id**—Outgoing Interface identifier.
- **metric**—Static route metric. Acceptable values are from 1 to 65535. The default value is 1.

Default Configuration

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Mode

Global Configuration

User Guidelines

If the next IPv6 address is a global IPv6 address, it should belong to a static on-link prefix. When an on-link prefix is removed or is changed to non on-link prefix, the static routes with next hop belonging to the prefix are removed from the configuration.

The *interface-if* argument can be defined only on a point-to-point interface.

Example

Example 1. The following example defines a static route with a global next hop:

```
ipv6 route 2001::/64 5::5
```

Example 2. The following example defines a static route on point-to-point tunnel 1:

```
ipv6 route 2001:DB8:2222::/48 tunnel1
```

Example 3. The following example defines a static route with a link-local next hop:

```
ipv6 route 2001:DB8:2222::/48 FE80::260:3EFF:FE11:6770%vlan1
```

49.31 ipv6 unicast-routing

Use the **ipv6 unicast-routing** command in Global Configuration mode to enable the forwarding of IPv6 Unicast datagrams.

To disable the forwarding of IPv6 Unicast datagrams, use the **no** form of this command.

Syntax

ipv6 unicast-routing

no ipv6 unicast-routing

Parameters

N/A.

Default Configuration

IPv6 Unicast routing is disabled.

Command Mode

Global Configuration

Example

The following example enables the forwarding of IPv6 Unicast datagrams:

```
ipv6 unicast-routing
```

49.32 ipv6 unreachables

Use the **ipv6 unreachables** command in Interface Configuration mode to enable the generation of Internet Control Message Protocol for IPv6 (ICMPv6) unreachable messages for any packets arriving on a specified interface.

To prevent the generation of unreachable messages, use the **no** form of this command.

Syntax

ipv6 unreachables

no ipv6 unreachables

Parameters

N/A.

Default Configuration

The sending of ICMP IPv6 unreachable messages is enabled.

Command Mode

Interface Configuration.

User Guidelines

If the switch receives a Unicast packet destined for itself that uses a protocol it does not recognize, it sends an ICMPv6 unreachable message to the source.

If the switch receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

Example

The following example disables the generation of ICMPv6 unreachable messages, as appropriate, on an interface:

```
interface vlan 100
  no ipv6 unreachables
exit
```

49.33 show ipv6 distance

Use the **show ipv6 distance** command in user EXEC or privileged EXEC mode to display the distance of the IPv6 routing protocols.

Syntax

show ipv6 distance

Parameters

N/A.

Command Mode

User EXEC

Privileged EXEC

Example

The following is sample output from the **show ipv6 distance** command:

```
show ipv6 distance
Protocol      Distance
-------       --------
connected          0
static             1
ospf intra-as     30
ospf inter-as    110
bgp external      20
bgp internal     200
bgp local        200
```

49.34 show ipv6 interface

Use the **show ipv6 interface** command in user EXEC or privileged EXEC mode to display the usability status of interfaces configured for IPv6.

Syntax

show ipv6 interface [**brief**] | [[*interface-id*] [**prefix**]]

Parameters

- **brief**—Displays a brief summary of IPv6 status and configuration for each interface where IPv6 is defined.
- **interface-id**—Interface identifier about which to display information.
- **prefix**—Prefix generated from a local IPv6 prefix pool.

Default Configuration

Option **brief** - all IPv6 interfaces are displayed.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use this command to validate the IPv6 status of an interface and its configured addresses. This command also displays the parameters that IPv6 uses for operation on this interface and any configured features.

If the interface’s hardware is usable, the interface is marked up.

If you specify an optional interface identifier, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

Example

Example 1. The show ipv6 interface command displays information about the specified interface:

```
show ipv6 interface vlan 1
VLAN 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
IPv6 Forwarding is enabled
Global unicast address(es):
Ipv6 Global Address                         Type
2000:0DB8::2/64 (ANY)                       Manual
2000:0DB8::2/64                             Manual
2000:1DB8::2011/64                          Manual
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router maximum advertisement interval is 600 seconds
ND router minimum advertisement interval is 198 seconds (DEFAULT)
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Stateless autoconfiguration is enabled.
MLD Version is 2
```

Field Descriptions:

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked Enabled. If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked Stalled. If IPv6 is not enabled, the interface is marked Disabled.
- **link-local address**—Displays the link-local address assigned to the interface.
- **Global unicast address(es):**—Displays the global Unicast addresses assigned to the interface. The type is **manual** or **autoconfig**.
- **Joined group address(es):**—Indicates the Multicast groups to which this interface belongs.
- —Maximum transmission unit of the interface.
- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
- **ICMP redirects**—State of ICMP IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled).
- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
- **ND advertised reachable time**—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
- **ND advertised retransmit interval**—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
- **ND router advertisements**—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.
- **ND advertised default router preference is Medium**—DRP for the router on a specific interface.
- **MLD Version**—Version of MLD

Example 2. The **show ipv6 interface command** displays information about the specified manual Ipv6 tunnel:

```
show ipv6 interface tunnel 2
Tunnel 2 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
IPv6 Forwarding is enabled
Global unicast address(es):
```

```
Ipv6 Global Address                         Type
2000:0DB8::2/64 (ANY)                       Manual
2000:0DB8::2/64                             Manual
2000:1DB8::2011/64                          Manual
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
MTU is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
MLD Version is 2
Tunnel mode is manual
Tunnel Local IPv4 address : 10.10.10.1(auto)
Tunnel Remote Ipv4 address : 10.1.1.1
```

Field Descriptions:

- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”
- **link-local address**—Displays the link-local address assigned to the interface.
- **Global Unicast address(es):**—Displays the global Unicast addresses assigned to the interface. The type is **manual** or **autoconfig**.
- **Joined group address(es):**—Indicates the Multicast groups to which this interface belongs.
- —Maximum transmission unit of the interface.
- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
- **ICMP redirects**—The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled).
- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.

- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
- **ND advertised reachable time**—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
- **ND advertised retransmit interval**—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
- **ND router advertisements**—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.
- **ND advertised default router preference is Medium**—The DRP for the router on a specific interface.
- **MLD Version**—The version of MLD
- **Tunnel Local IPv4 address**—Specifies the tunnel local IPv4 address and have one of the following formats:
  - *ipv4-address*
  - *ipv4-address* (auto)
  - *ipv4-address* (*interface-id*)
- **Tunnel Remote Ipv4 address**—Specifies the tunnel remote IPv4 address

Example 3. The **show ipv6 interface** command displays information about the specified tunnel:

```
show ipv6 interface tunnel 1
Tunnel 1 is up/up
IPv6 is enabled, link-local address is FE80::0DB8:12AB:FA01
ICMP redirects are disabled
Global unicast address(es):
Ipv6 Global Address                         Type
2000:0DB8::2/64 (ANY)                       Manual
2000:0DB8::2/64                             Manual
2000:1DB8::2011/64                          Manual
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF11:6770
 is 1500 bytes
ICMP error messages limited interval is 100ms; Bucket size is 10 tokens
ICMP redirects are enabled
ND DAD is disabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

```
MLD Version is 2
Tunnel Local IPv4 address : 10.10.10.1(VLAN 1)
```

Field Descriptions:

- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled). **Note.** The switch will enable DAD automatically when the user change the type of the tunnel to manual if a the parameter value bigger than 0.
- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
- **vlan 1 is up/up**—Indicates the interface status: administrative/operational.
- **IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)**—Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.”
- **link-local address**—Displays the link-local address assigned to the interface.
- **Global Unicast address(es):**—Displays the global Unicast addresses assigned to the interface. The type is **manual** or **autoconfig**.
- **Joined group address(es):**—Indicates the Multicast groups to which this interface belongs.
- —Maximum transmission unit of the interface.
- **ICMP error messages**—Specifies the minimum interval (in milliseconds) between error messages sent on this interface.
- **ICMP redirects**—The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).
- **number of DAD attempts:**—Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed.
- **ND reachable time**—Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface.
- **ND advertised reachable time**—Displays the neighbor discovery reachable time (in milliseconds) advertised on this interface.
- **ND advertised retransmit interval**—Displays the neighbor discovery retransmit interval (in milliseconds) advertised on this interface.
- **ND router advertisements**—Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire.
- **ND advertised default router preference is Medium**—The DRP for the router on a specific interface.
- **MLD Version**—The version of MLD
- **Tunnel Local IPv4 address**—Specifies the tunnel local IPv4 address and have one of the following formats:
  - *ipv4-address*
  - *ipv4-address* (auto)
  - *ipv4-address* (*interface-id*)
- **Tunnel Remote Ipv4 address**—Specifies the tunnel remote IPv4 address

Example 4. The following command with the **brief** keyword displays information about all interfaces that IPv6 is defined on:

```
Router# show ipv6 interface brief
Interface         Interface IPv6     Link Local         MLD        Number of
```

```
                  State     State     IPv6 Address      Version  Global Addresses
----------------- --------- -------  ----------------- ------   ----------------
fa1/0/10          up/up     enabled  FE80::0DB8:12AB:FA01   1              1
fa1/0/11          up/up     stalled  FE80::0DB8:12AB:FA01   1              1
fa1/0/12          up/down   enabled  FE80::0DB8:12AB:FA01   1              3
po1               down/down enabled  FE80::0DB8:12AB:FA01   2              2
tunnel 1          up/up     enabled  FE80::0DB8:12AB:FA01   1              1
vlan 1            up/up     enabled  FE80::0DB8:12AB:FA01   1              1
vlan 1000         up/up     stalled  FE80::0DB8:12AB:FA01   1              1
```

Example 5. This sample output shows the characteristics of VLAN 1 that has generated a prefix from a local IPv6 prefix pool:

```
interface vlan1
  ipv6 address 2001:0DB8:1::1/64
  ipv6 address 2001:0DB8:2::1/64
  ipv6 address 2001:0DB8:3::1/64
  ipv6 nd prefix 2001:0DB8:1::/64 no-advertise
  ipv6 nd prefix 2001:0DB8:3::/64 2912000 564900 off-link
  ipv6 nd prefix 2001:0DB8:4::/64
  ipv6 nd prefix 2001:0DB8:5::/64 2912000 564900 off-link
exit
.
.
.
show ipv6 interface vlan 1 prefix
IPv6 Prefix Advertisements VLAN 1
Codes: A - Address, P - Prefix is advertised, R is in Routing Table
Code Prefix               Flags  Valid Lifetime    Preferred Lifetime
---- ----------------     ----  ---------------    -----------------------
     default              LA      2592000          604800
AR   2001:0DB8:1::/64     LA      infinite         infinite
APR  2001:0DB8:2::/64     LA      infinite         infinite
AP   2001:0DB8:3::/64     A       infinite         infinite
PR   2001:0DB8:4::/64     LA      2592000          604800
P    2001:0DB8:5::/64     A       2912000          564900
```

49.35 show ipv6 link-local default zone

Use the **show ipv6 link-local default zone** command in user EXEC or privileged EXEC mode to display the IPv6 link local default zone.

Syntax

show ipv6 link-local default zone

Command Mode

EXEC mode

Privileged EXEC

Example

Example 1. The following example displays the default zone when it is defined:

```
show ipv6 link-local default zone
Link Local Default Zone is VLAN 1
```

Example 2. The following example displays the default zone when it is not defined:

```
show ipv6 link-local default zone
Link Local Default Zone is not defined
```

49.36 show ipv6 nd prefix

Use the **show ipv6 nd prefix** command in user EXEC or privileged EXEC mode to display IPv6 prefixes included in IPv6 Neighbor Discovery (ND) router advertisements.

Syntax

show ipv6 nd prefix [*interface-id*]

Parameters

interface-id—Specified interface identifier on which prefixes are advertised.

Default Configuration

No prefixes are displayed.

Command Mode

EXEC mode

Privileged EXEC

User Guidelines

Use the **how ipv6 nd prefix** command with the *interface-id* argument to display prefixes advertised on a single interface.

Example

The following example displays active SeND certificates:

```
show ipv6 nd prefix vlan 100
vlan 100
```

```
default
  valid-lifetime 2,592,000 secs
  preferred-lifetime 604,800 secs
  on-link
  auto-config
prefix 2001::1/64
  valid-lifetime 3,600 secs
  preferred-lifetime 2,700 secs
prefix 2001:2:12/64
  no advertise
prefix 2002::1/64
  valid-lifetime 3,600 secs
  preferred-lifetime 2,700 secs
  on-link
prefix 2011::1/64
  valid-lifetime 3,600 secs
  preferred-lifetime 2,700 secs
  off-link
  auto-config
```

49.37 show ipv6 neighbors

Use the **show ipv6 neighbors** command in User EXEC or Privileged EXEC mode to display IPv6 neighbor discovery (ND) cache information.

Syntax

show ipv6 neighbors [*interface-id* | *ipv6-address* | *ipv6-hostname*]

Parameters

- **interface-id**—Specifies the identifier of the interface from which IPv6 neighbor information is to be displayed.
- **ipv6-address**—Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **ipv6-hostname**—Specifies the IPv6 host name of the remote networking device.

Default Configuration

All IPv6 ND cache entries are listed.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

When the *interface-id* argument is not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-id* argument displays only cache information about the specified interface.

Example

Example 1. The following is sample output from the show ipv6 neighbors command when entered with an interface-id:

```
show ipv6 neighbors vlan 1
IPv6 Address               Age Link-layer Addr     State  Interface Router
2000:0:0:4::2               0    0003.a0d6.141e    REACH  VLAN1       Yes
3001:1::45a                 -    0002.7d1a.9472    REACH  VLAN1       -
FE80::203:A0FF:FED6:141E    0    0003.a0d6.141e    REACH  VLAN1       No
```

Example 2. The following is sample output from the show ipv6 neighbors command when entered with an IPv6 address:

```
show ipv6 neighbors 2000:0:0:4::2
IPv6 Address               Age Link-layer Addr     State  Interface Router
2000:0:0:4::2               0    0003.a0d6.141e    REACH  VLAN1       Yes
```

Field Descriptions:

- **Total number of entries**—Number of entries (peers) in the cache.
- **IPv6 Address**—IPv6 address of neighbor or interface.
- **Age**—Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- **Link-layer Addr**—MAC address. If the address is unknown, a hyphen (-) is displayed.
- **Interface**—Interface which the neighbor is connected to.
- **Router**—Specifies if the neighbor is a Router. A hyphen (-) is displayed for static entries.

49.38 show ipv6 prefix-list

Use the **show ipv6 prefix-list** command in user EXEC or privileged EXEC mode. to display information about an IPv6 prefix list or IPv6 prefix list entries.

Syntax

show ipv6 prefix-list [**detail** [*list-name*] | **summary** [*list-name*]]

show ipv6 prefix-list *list-name ipv6-prefix*/*prefix-length* [**longer** | **first-match**]

show ipv6 prefix-list *list-name* **seq** *seq-num*

Parameters

- **detail | summary**—Displays detailed or summarized information about all IPv6 prefix lists.
- **list-name**—Name of a specific IPv6 prefix list.
- **ipv6-prefix**—All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal using 16-bit values between colons.

- **/prefix-length**—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 value.
- **longer**—Displays all entries of an IPv6 prefix list that are more specific than the given ipv6-prefix/prefix-length values.
- **first-match**—Displays the entry of an IPv6 prefix list that matches the given ipv6-prefix/prefix-length values.
- **seq** *seq-num*—Sequence number of the IPv6 prefix list entry.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

This command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

If the **detail** and **summary** keywords are omitted, the **detail** option is applied.

If the **longer** and f**irst-match** keywords are omitted, all entries of the specified prefix list that matches the given network/length are displayed.

Example

Example 1. The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
show ipv6 prefix-list detail
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
  seq 5 permit 2002::/16 (hit count: 313)
ipv6 prefix-list aggregate:
  count: 3, range entries: 2
  seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568)
  seq 10 description The Default Action
  seq 15 permit ::/0 le 48 (hit count: 31310)
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3
  seq 5 deny 5F00::/8 le 128 (hit count: 0)
  seq 10 deny ::/0 (hit count: 0)
  seq 15 deny ::/1 (hit count: 0)
  seq 20 deny ::/2 (hit count: 0)
  seq 25 deny ::/3 ge 4 (hit count: 0)
  seq 30 permit ::/0 le 128 (hit count: 240664)
```

Field Descriptions

- **count**—Number of entries in the list.
- **range entries**—Number of entries with matching range.

- **seq**—Entry number in the list.
- **permit, deny**—Granting status.
- **description**—Comment.
- **hit count**—Number of matches for the prefix entry.

Example 2. The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword:

```
show ipv6 prefix-list summary
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
ipv6 prefix-list aggregate:
  count: 2, range entries: 2
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3
```

Example 3. The following example shows the output of the **show ipv6 prefix-list** command with the **seq** keyword:

```
show ipv6 prefix-list bgp-in seq 15

  seq 15 deny ::/1 (hit count: 0)
```

49.39 show ipv6 protocols

Use the **show ipv6 protocols** command in User EXEC or Privileged EXEC mode to display the parameters and current state of the active IPv6 routing protocol processes.

Syntax

show ipv6 protocols [**summary**]

Parameters

summary—Displays the configured routing protocol process names.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The information displayed by this command is useful in debugging routing operations.

Example

Example 1. The following is sample output from the **show ipv6 protocols** command, showing active routing protocols:

```
show ipv6 protocols ospf
```

```
IPv6 Routing Protocol is "ospf 1"
  Interfaces:
    VLAN 3
    VLAN 100
    Tunnel 1
IPv6 Routing Protocol is "ospf 10"
  Interfaces:
    VLAN 10
    VLAN 130
    Tunnel 2
```

Field Descriptions

- **IPv6 Routing Protocol is**—Specifies the IPv6 routing protocol used and process-id.
- **Interfaces**—Specifies the interfaces on which the routing protocol is configured.

Example 2. The following is sample output from the show ipv6 protocols command with the **summary** keyword:

```
show ipv6 protocols summary
IPv6 Routing Protocol is "ospf 1"
IPv6 Routing Protocol is "ospf 10"
```

49.40 show ipv6 route

Use the **show ipv6 route** command in user EXEC or privileged EXEC mode to display the current contents of the IPv6 routing table.

Syntax

show ipv6 route [*ipv6-address* | *ipv6-prefix/prefix-length* | *protocol* | **interface** *interface-id*]

Parameters

- **ipv6-address**—Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **ipv6-prefix**—Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—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 value.
- **protocol**—Displays routes for the specified routing protocol using any of these keywords: **bgp**, **isis**, **ospf**, or **rip**; or displays routes for the specified type of route using any of these keywords: **connected**, **static**, **nd**, or **icmp**.
- **interface** *interface-id*—Identifier of an interface.

Default Configuration

All IPv6 routing information for all active routing tables is displayed.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

This command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. When the **icmp**, **nd**, **connected**, **local**, or **static** keywords are specified, only that type of route is displayed. When the *interface-id* argument are specified, only the specified interface-specific routes are displayed.

Example

Example 1. The following is sample output from the **show ipv6 route** command when IPv6 Routing is not enabled and the command is entered without an IPv6 address or prefix specified:

```
show ipv6 route
Codes: > - Best
       S - Static, I - ICMP Redirect, ND - Router Advertisment
[d/m]: d - route’s distance, m - route’s metric

IPv6 Routing Table - 6 entries
S> ::/0 [1/1]
   via fe80::77  VLAN 1
ND> ::/0   [11/0]
   via fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
ND> 2001::/64 [0/0]
   via ::  VLAN 100
ND> 2002:1:1:1::/64 [0/0]
   via ::  VLAN 100
ND> 3001::/64 [0/0]
    via ::  VLAN 101
ND> 4004::/64 [0/0]
     via ::  VLAN 110
```

Example 2. The following is sample output from the **show ipv6 route** command when IPv6 Routing is supported and the command is entered without an IPv6 address or prefix specified and IPv6 Routing is enabled:

```
show ipv6 route
Codes: > - Best
    I - ICMP Redirect, S - Static, C - Connected,
    L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link
        keyword,
    O - OSPF intra-area, OIA - OSPF inter-area,
    OE1 - OSPF external 1, OE2 - OSPF external 2,
    B - BGP
[d/m]: d - route’s distance, m - route’s metric

IPv6 Routing Table - 5 entries
B>   3000::/64 [20/0]
       via FE80::A8BB:CCFF:FE02:8B00   VLAN 100
OE1> 4000::2/128 [0/0]
       via FE80::A8BB:CCFF:FE02:8B01   VLAN 101
O>   4000::/64 [0/0]
       via FE80::A8BB:CCFF:FE02:8B02   VLAN 101
C>   4001::/64 [0/0]
       via ::   VLAN 100
L>   4002::/64 [0/0]
       via ::   VLAN 100 Lifetime 9000 sec
```

Example 3. The following is sample output from the show ipv6 route command when entered with the IPv6 prefix 2001:200::/35 and IPv6 Routing is supported:

```
show ipv6 route 2001:200::/35
Codes: > - Best
    I - ICMP Redirect, S - Static, C - Connected,
    L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link
        keyword,
    O - OSPF intra-area, OIA - OSPF inter-area,
    OE1 - OSPF external 1, OE2 - OSPF external 2,
    B - BGP
[d/m]: d - route’s distance, m - route’s metric

IPv6 Routing Table - 261 entries
OE1>   2001:200::/35 [20/3]
       via FE80::60:5C59:9E00:16 Tunnel1
```

Example 4. The following is sample output from the show ipv6 route command when IPv6 Routing is supported and the command is entered with the bgp keyword:

```
show ipv6 route bgp
Codes: > - Best
    I - ICMP Redirect, S - Static, C - Connected,
    L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link
        keyword,
    O - OSPF intra-area, OIA - OSPF inter-area,
    OE1 - OSPF external 1, OE2 - OSPF external 2,
    B - BGP
[d/m]: d - route’s distance, m - route’s metric

IPv6 Routing Table - 129 entries
B>  3000::/64 [20/0]
       via FE80::A8BB:CCFF:FE02:8B00 Tunnel1
```

49.41 show ipv6 route summary

Use the **show ipv6 route summary** command in User EXEC or Privileged EXEC mode to display the current contents of the IPv6 routing table in summary format.

Syntax

show ipv6 route summary

Parameters

N/A.

Command Mode

User EXEC

Privileged EXEC

Example

The following is sample output from the show ipv6 route summary command:

```
show ipv6 route summary
IPv6 Routing Table Summary - 97 entries
37 local, 35 connected, 25 static
Number of prefixes:
/16: 1, /28: 10, /32: 5, /35: 25, /40: 1, /64: 9
/96: 5, /112: 1, /127: 4, /128: 36
```

49.42 show ipv6 static

Use the **show ipv6 static** command in user EXEC or privileged EXEC mode to display the current static routes of the IPv6 routing table.

Syntax

show ipv6 static [*ipv6-address* | *ipv6-prefix/prefix-length*] [**interface** *interface-id*][**detail**]

Parameters

- **ipv6-address**—Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **ipv6-prefix**—Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC4293 where the address is specified in hexadecimal using 16-bit values between colons.
- **/prefix-length**—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 value.
- **interface** *interface-id*—Identifier of an interface.
- **detail**—Specifies for invalid routes, the reason why the route is not valid.

Default Configuration

All IPv6 static routing information for all active routing tables is displayed.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

When the *ipv6-address* or *ipv6-prefix*/*prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the *interface-id* argument is specified, only the specified interface-specific routes are displayed.

When the **detail** keyword is specified, the reason why the route is not valid is displayed for invalid direct or fully specified routes.

Example

Example 1. The following is sample output from the **show ipv6 static** command without specified options:

```
show ipv6 static
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface VLAN2, metric 1
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
```

Example 2. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
show ipv6 static 2001:200::/35
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 2001:200::/35, via nexthop 4000::1, metric 1
   2001:200::/35, via nexthop 9999::1, metric 1
* 2001:200::/35, interface VLAN1, metric 1
```

Example 3. The following is sample output from the **show ipv6 route** command when entered with the interface VLAN 1:

```
show ipv6 static interface vlan 1
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 5000::/16, interface VLAN1, metric 1
```

Example 4. The following is sample output from the **show ipv6 route** command with the **detail** keyword:

```
show ipv6 static detail
IPv6 Static routes   Code: * - installed in Routing Information Base (RIB)
IPv6 Static routes distance is 1
* 3000::/16, interface VLAN1, metric 1
* 4000::/16, via nexthop 2001:1::1, metric 1
  5000::/16, interface fa 1/0/10, metric 1
         Interface is down
* 5555::/16, via nexthop 4000::1, metric 1
  5555::/16, via nexthop 9999::1, metric 1
         Route does not fully resolve
* 5555::/16, via nexthop 4001:AF00::1, metric 1
* 6000::/16, via nexthop 2007::1, metric 1
```

50 OpenFlow Commands

50.1 openflow enable

Use the **openflow enable** Global Configuration mode command to enable the OpenFlow feature. Use the **no** form of this command to disable this feature.

Syntax

openflow enable

no openflow enable

Parameters

N/A

Default Configuration

Openflow is enabled.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the device.

Example

The following example enables OpenFlow

```
switchxxxxxx(config)# openflow enable
```

50.2 openflow forward_action

Use the **openflow forward action** Global Configuration command to determine the default rule for non-matched flows.

Use the **no** form of this command to return to the default forward action.

Syntax

openflow forward_action *[forward* | *drop* | *to_controller}*

no openflow forward_action

Parameters

- **forward**—Forward unmatched packets based on regular bridging rules
- **drop**—Drop unmatched packets
- **to_controller**—Forward unmatched packets to the OpenFlow controller

Default Configuration

Default configuration is to_controller.

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the device

Example

```
switchxxxxxx(config)# openflow forward_action drop
```

50.3 openflow ip-address

Use the **openflow ip-address** Global Configuration mode command to configure the OpenFlow controller IP.

Use the **no** form of this command to restore the default.

Syntax

openflow ip-address *ip-address*

no openflow *ip-address*

Parameters

ip-address—Specifies the IP address of the OpenFlow controller

Default Configuration

10.10.10.10

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the device.

Example

```
switchxxxxxx(config)# openflow ip-address 192.168.1.1
```

50.4 openflow protocol

Use the **openflow protocol** Global Configuration mode command to configure the OpenFlow protocol and the port number in the connection to the OpenFlow controller.

Use the **no** form of this command to set the default protocol and port.

Syntax

openflow protocol tcp { **tcp-port** [*port-id*] }

no openflow protocol

Parameters

- **tcp-port** [*port-id*]—Specifies the TCP port that will be used in the communication with the OpenFlow controller.

Default Configuration

TCP port 6633

Command Mode

Global Configuration mode

User Guidelines

This command takes effect only after resetting the device.

Example

```
switchxxxxxx(config)# openflow protocol tcp tcp-port 1234
```

50.5 show openflow

Use the **show openflow** Exec mode command to display the OpenFlow configuration on the device.

Syntax

show openflow

Parameters

N/A

Command Mode

Privileged EXEC mode

Example

The following example shows the output of this command.

```
switchxxxxxx#show openflow
OpenFlow status: Enabled
OpenFlow status after reset: Enabled
OpenFlow protocol: tcp
OpenFlow TCP port:  6633
OpenFlow Server IP Address: 10.10.10.10
OpenFlow OOB Server IP Address: 10.10.10.10
OpenFlow Default Forward Action: toController
```

51 Open Shortest Path First for IPv6(OSPFv3) Commands

51.1 area default-cost

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the **area default-cost** command in router address family topology or router configuration mode. To return to default, use the **no** form of this command.

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameters

- **area-id**—Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
- **cost**—Cost for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number.

Default Configuration

cost—1.

Command Mode

Router configuration (config-router)

User Guidelines

If the area does not exist when the **area default-cost** command is applied it is created.

This command is used only on an Area Border Router (ABR) attached to a stub area or NSSA. If the area is not a stub area or NSSA or the Router is not an ABR attached to the stub area or NSSA then the configuration is saved but is not applied.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers attached to the stub area, the area should be configured as a stub area using the **area stub** command. The **area default-cost** command impacts only on an ABR attached to the stub area. If the **area default-cost** command is configured on non ABR attached to the area the configuration is saved but it is not applied. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Note. To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
ipv6 router ospf 1
```

```
 area 10.0.0.0 stub
 area 10.0.0.0 default-cost 20
exit
```

51.2 area filter-list

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the **area filter-list** command in router configuration mode. To cancel the filter, use the **no** form of this command.

Syntax

area *area-id* **filter-list prefix** *prefix-list-name* {**in** | **out**}

no area *area-id* **filter-list prefix** {**in** | **out**}

Parameters

- **area-id**—Identifier of the area for which filtering is configured. The identifier can be specified as either a decimal value or an IP address.
- **prefix-list-name**—Name of an IPv6 prefix list.
- **in**—The prefix list is applied to prefixes advertised to the specified area from other areas.
- **out**—The prefix list is applied to prefixes advertised out of the specified area to other areas.

Default Configuration

This command is disabled by default. The router will not filter prefixes.

Command Mode

Router configuration (config-router)

User Guidelines

If the area does not exist when the **area filter-list** command is applied it is created.

The **area filter-list** command impacts only on an ABR. If the **area filter-list** command is configured on non ABR the configuration is saved but it is not applied.

With this feature enabled in the "**in**" direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the **area range** command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.

With this feature enabled in the "**out**" direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the **area range** command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if at least one prefix in the area range matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the **area range** command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

Example

The following example filters prefixes that are sent from all other areas to area 1:

```
area 1 filter-list prefix AREA_1 in
```

51.3 area nssa

To configure a not-so-stubby area (NSSA), use the **area nssa** command in router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

Syntax

area *area-id* **nssa** [**no-summary**] [**translator-role** {**always** | **candidate**}] [**translator-stability-interval** *seconds*]

no area *area-id* **nssa**

Parameters

- **area-id**—Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.
- **no-summary**—Allows an area to be an NSSA but not have summary routes injected into it.
- **translator-role**—Specifies whether or not an NSSA border router will unconditionally translate Type-7 LSAs into Type-5 LSAs. The default value is **candidate**.
- **always**—Specifies that an NSSA border router always translates Type-7 LSAs into Type-5 LSAs regardless of the translator state of other NSSA border routers.
- **candidate**—Specifies that an NSSA border router participates in the translator election process described in RFC 3101, Section 3.1.
- **seconds**—Specifies the number of seconds after an elected translator determines its services are no longer required, that it should continue to perform its translation duties. The default value is 40 seconds.

Default Configuration

No NSSA area is defined.

Command Mode

Router configuration (config-router)

User Guidelines

If the area does not exist when the **area nssa** command is applied it is created.

The **no** format of the **area nssa** command does not remove the area, it only changes the area type to transit.

To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, including **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

The following example makes area 1 an NSSA area:

```
ipv6 router ospf 1
 area 1 nssa
exit
```

51.4 area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

Syntax

area *area-id* **range** *ipv6-prefix /prefix-length* [**advertise** | **not-advertise**]

no area *area-id* **range** i*pv6-prefix* **/***prefix-length*

Parameters

- **area-id**—Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.
- **ipv6-prefix**—IPv6 prefix.
- **/prefix-length**—IPv6 prefix length.
- **advertise**—Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
- **not-advertise**—Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Default Configuration

This command is disabled by default.

Command Mode

Router configuration

User Guidelines

The **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*.

If the [**advertise** | **not-advertise**] keywords are not defined then the **advertise** option is applied by default.

Multiple area router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note. To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 2001:0DB8:0:1::/64:

```
interface vlan 100
 ipv6 enable
 ipv6 ospf 1 area 1
exit
ipv6 router ospf 1
```

```
 router-id 192.168.255.5
 area 1 range 2001:0DB8:0:1::/64
exit
```

51.5 area shutdown

To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol in the current area, use the **area shutdown** command in router configuration mode. To restart the OSPF protocol, use the **no** form of this command.

Syntax

area *area-id* **shutdown**

no area *area-id* **shutdown**

Parameters

area-id—Identifier for the area. The identifier can be specified as either a decimal value or an IP address.

Default Configuration

OSPF stays active in the current area.

Command Mode

Router configuration (config-router)

User Guidelines

Use the **area shutdown** command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.

Example

The following example shows how to enable a graceful shutdown of the OSPF protocol in area 10.0.0.0:

```
ipv6 router ospf 1
 area 10.0.0.0 shutdown
exit
```

51.6 area stub

To define an area as a stub area, use the **area stub** command in router address family topology or router configuration mode. To disable this function, use the **no** form of this command.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub**

Parameters

- **area-id**—Identifier for the stub area. The identifier can be specified as either a decimal value or an IP address.
- **no-summary**—Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Default Configuration

No stub area is defined.

Command Mode

Router configuration (config-router)

User Guidelines

If the area does not exist when the **area stub** command is configured it is created.

The **no** format of the **area stub** command does not remove the area, it only changes the area type to transit.

You must configure the **area stub** command on all routers and access servers in the stub area. Use the **area** router configuration command with the **default-cost** keyword to specify the cost of a default internal route sent into a stub area by an ABR.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers attached to the stub area, the area should be configured as a stub area using the **area stub** command. The **area default-cost** command is needed only on an ABR attached to the stub area. If the **area default-cost** command is configured on non ABR attached to the area the configuration is saved but is not effected. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area. The **no-summary** keyword configured on non ABR is saved but is not effected.

Note. To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
ipv6 router ospf
  area 10.0.0.0 default-cost 20
  area 10.0.0.0 stub
exit
```

51.7 area virtual-link

To define an Open Shortest Path First (OSPF) virtual link, use the **area virtual-link** command in router address family topology or router configuration mode. To remove a virtual link, use the **no** form of this command.

Syntax

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*]

no area *area-id* **virtual-link** *router-id*

Parameters

- **area-id**—Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.
- **router-id**—Router ID associated with the virtual link neighbor. The router ID appears in the **show ip ospf** or **show ipv6 display** command. There is no default.
- **hello-interval** *seconds*—Time (in seconds) between the hello packets that the software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. Range is from 1 to 8192. The default is 10.
- **retransmit-interval** *seconds*—Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. Range is from 1 to 8192. The default is 5.
- **transmit-delay** *seconds*—Estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. Range is from 1 to 8192. The default value is 1.
- **dead-interval** *seconds*—Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.

Default Configuration

No OSPF virtual link is defined.

Command Mode

Router configuration (config-router)

User Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Note. In order for a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the show ip ospf or the show ipv6 ospf command in privileged EXEC mode.

Note. To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

Example 1. The following example establishes a virtual link with default values for all optional parameters:

```
ipv6 router ospf 1
 area 1 virtual-link 192.168.255.1
exit
```

Example 2. The following example establishes a virtual link in OSPF for IPv6:

```
ipv6 router ospf 1
 area 1 virtual-link 192.168.255.1 hello-interval 5
exit
```

51.8 clear ipv6 ospf process

To restart the Open Shortest Path First (OSPF) process, use the **clear ipv6 ospf process** command in privileged EXEC mode.

Syntax

clear ipv6 ospf [*process-id*] **process**

Parameters

process-id—Process ID. If the parameter is omitted all the OSPF processes are restarted.

Default Configuration

N/A

Command Mode

Privileged EXEC

User Guidelines

Use the *process-id* argument to restart only one OSPF process. If the *process-id* argument is not specified, all OSPF processes are restarted.

The **clear ipv6 ospf process** command changes the OSPF process router-id if it was reconfigured by the user else if the current used router-id has the default value the command runs the router-id re-election algorithm.

Example

Example 1. The following example restarts all the OSP processes:

```
clear ipv6 ospf process
```

Example 2. The following example restarts one OSP process with process-id 1:

```
clear ipv6 ospf 1 process
```

51.9 default-metric (IPv6 OSPF)

To set default metric values for routes redistributed into the Open Shortest Path First (OSPF) for IPv6 routing protocol, use the **default-metric command** in router configuration mode. To return to the default state, use the **no** form of this command.

Syntax

default-metric *metric-value*

no default-metric

Parameters

metric-value—Default metric value appropriate for the specified routing protocol. The range is from 1 to 4294967295.

Default Configuration

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router configuration

User Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Finer control over the metrics of reditributed routes can be gained by using the options to the **redistribute** command, including route maps.

Example

The following example shows an OSPF for IPv6 routing protocol redistributing routes from the Routing Information Protocol (RIP). All the redistributed routes are advertised with a metric of 10:

```
ipv6 router ospf 100
  default-metric 10
  redistribute rip
exit
```

51.10 ipv6 ospf area

To enable OSPF for IPv6 on an interface, use the **ipv6 ospf area** command in interface configuration mode. To disable OSPF routing for interfaces defined, use the **no** form of this command.

Syntax

ipv6 ospf *process-id* **area** *area-id* [**shutdown**]

no ipv6 ospf *process-id* **area** *area-id*

Parameters

- **process-id**—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process. The number must be in range 1-255.
- **area-id**—Area that is to be associated with the OSPF interface.
- **shutdown**—OSPF is enabled on the interface in the shutdown state.

Default Configuration

OSPF for IPv6 is disabled.

Command Mode

Interface configuration

User Guidelines

Before you enable OSPF for IPv6 on an interface using the i**pv6 ospf area** command, you must enable IPv6 on the interface.

If the OSPFv3 process has not be created it is created automatically.

In IPv6, users can configure many addresses on an interface. In OSPF for IPv6, all addresses on an interface are included by default. Users cannot select some addresses to be imported into OSPF for IPv6; either all addresses on an interface are imported, or no addresses on an interface are imported.

Use the **ipv6 ospf area** command with the **shutdown** keyword to create OSPFv3 process on an interface if you are going to change the default values of OSPF configuration and the use the **no ipv6 ospf shutdown** command.

There is no limit to the number of **ipv6 ospf area** commands you can use on the router. You must have at least two interfaces configured for OSPF for IPv6 to run.

Example

The following example enables OSPF for IPv6 on an interface:

```
ipv6 unicast-routing
interface vlan 100
  ipv6 enable
  ipv6 ospf 1 area 0
exit
interface vlan 200
  ipv6 enable
  ipv6 ospf 120 area 1.4.20.9
exit
```

51.11 ipv6 ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ipv6 ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

Syntax

ipv6 ospf cost *interface-cost*

no ipv6 ospf cost

Parameters

interface-cost—Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.

Default Configuration

The default value depends on the interface's ifSpeed (see **User Guidelines**).

Command Mode

Interface configuration

User Guidelines

You must define OSPFv3 on an interface by the **ipv6 ospf area** command before using of the **ipv6 ospf cost** command on the same interface.

You can set the metric manually using this command, if you need to change the default.

In general, the path cost is calculated using the following formula:

10^10 / ifSpeed

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

10G Ethernet Default cost is 1

1G Ethernet Default cost is 10

100M Ethernet Default cost is 100

10M Ethernet Default cost is 1000

Example

The following example sets the interface cost value to 65:

```
ipv6 ospf cost 65
```

51.12 ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

Syntax

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval

Parameters

seconds—Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network.

Default Configuration

Four times the interval set by the **ipv6 ospf hello-interval** command.

Command Mode

Interface configuration

User Guidelines

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Example

The following example sets the Open Shortest Path First (OSPF) dead interval to 60 seconds:

```
interface vlan 100
  ipv6 ospf dead-interval 60
exit
```

51.13 ipv6 ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the **ipv6 ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

Syntax

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

Parameters

seconds—Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

Default Configuration

10 seconds

Command Mode

Interface configuration

User Guidelines

This value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Example

The following example sets the interval between hello packets to 15 seconds:

```
interface vlan 100
  ipv6 ospf hello-interval 15
exit
```

51.14 ipv6 ospf mtu-ignore

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ipv6 ospf mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Parameters

This command has no arguments or keywords.

Default Configuration

This command is disabled.

Command Mode

Interface configuration

User Guidelines

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher then the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Example

The following example disables MTU mismatch detection on receiving DBD packets:

```
interface vlan 100
  ipv6 ospf mtu-ignore
exit
```

51.15 ipv6 ospf neighbor

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **ipv6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

Syntax

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] **no ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] Parameters

ipv6-address—Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

priority *number*—A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified. The default is 0.

poll-interval *seconds*—A number value that represents the poll interval time (in seconds). RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.

cost *number*—Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ipv6 ospf cost command.

Default Configuration

No configuration is specified.

Command Mode

Interface configuration

User Guidelines

One neighbor entry must be included in the configuration for each known nonbroadcast network neighbor. The neighbor address must be a link-local address of the neighbor.

If a neighboring router has become inactive (hello packets have not been seen for the Router Dead Interval period), hello packets may need to be sent to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

The **priority** keyword does not apply to point-to-multipoint interfaces. For point-to-multipoint interfaces, the **cost** keyword and the *number* argument are the only options that are applicable. The **cost** keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

Example

The following example configures an OSPF neighboring router:

```
interface tunnel 4
  ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
exit
```

51.16 ipv6 ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ipv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

Syntax

ipv6 ospf priority *number-value*

no ipv6 ospf priority

Parameters

number-value—A number value that specifies the priority of the router. The range is from 0 to 255.

Default Configuration

The router priority is 1.

Command Mode

Interface configuration

User Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First (OSPF) for nonbroadcast networks using the **ipv6 ospf neighbor** command.

Example

The following example sets the router priority value to 4:

```
interface vlan 100
  ipv6 ospf priority 4
exit
```

51.17 ipv6 ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ipv6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

Syntax

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval

Parameters

seconds—Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.

Default Configuration

The default is 5 seconds.

Command Mode

Interface configuration

User Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Example

The following example sets the retransmit interval value to 8 seconds:

```
interface vlan 100
  ipv6 ospf retransmit-interval 8
exit
```

51.18 ipv6 ospf shutdown

To initiate an Open Shortest Path First (OSPF) for IPv6 protocol graceful shutdown at the interface level, use the **ipv6 ospf shutdown** command in interface configuration mode. To restart the OSPF protocol on an interface, use the **no** form of this command.

Syntax

ip ospf shutdown

no ip ospf shutdown

Parameters

N/A

Default Configuration

N/A

Command Mode

Interface configuration

User Guidelines

Use the **ipv6 ospf shutdown** command to put OSPF on a specific interface in shutdown mode.

Example

The following example shows how to initiate an OSPF protocol shutdown on IP interface 1.1.1.1:

```
interface vlan 100
  ip ospf shutdown
exit
```

51.19 ipv6 ospf transmit-delay

To set the estimated time required to send a link-state update packet on the interface, use the **ip ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

Syntax

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

Parameters

seconds—Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Default Configuration

The default is 1 second.

Command Mode

Interface configuration

User Guidelines

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Example

The following example sets the retransmit delay value to 3 seconds:

```
interface vlan 100
  ipv6 ospf transmit-delay 3
exit
```

51.20 ipv6 router ospf

To enable Open Shortest Path First (OSPF) for IPv6 router configuration mode, use the **ipv6 router ospf** command in global configuration mode.

Syntax

ipv6 router ospf *process-id*

Parameters

process-id—Internal identification. It is locally assigned and can be a positive integer from 1 to 255. The number used here is the number assigned administratively when enabling the OSPF for IPv6 routing process.

Default Configuration

No OSPF for IPv6 routing process is defined.

Command Mode

Global configuration

User Guidelines

Use this command to enter the OSPF for IPv6 router configuration mode. If the OSPFv3 process has not been created it is created. From this mode, you can enter several commands to customize OSPF for IPv6.

Example

The following example enables router OSPF for IPv6 configuration mode and identifies the process with the number 1:

```
ipv6 router ospf 1
```

51.21 no area

To remove the specified area from the software configuration, use the **no area** command in router configuration mode.

Syntax

no area *area-id*

Parameters

area-id—Identifier for the removed area. The identifier can be specified as either a decimal value or an IP address.

Default Configuration

Area is defined.

Command Mode

Router configuration (config-router)

User Guidelines

To remove the specified area from the software configuration, use the **no area** *area-id* command. That is, the **no area** *area-id* command removes all area options, including **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

The following example removes area 1:

```
ipv6 router ospf 1
 no area 1
exit
```

51.22 passive-interface (IPv6)

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

Syntax

passive-interface [**default** | *interface-id*]

no passive-interface [**default** | *interface-id*]

Parameters

- **default**—All interfaces become passive.

- **interface-id**—Interface identifier.

Default Configuration

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Mode

Router configuration

User Guidelines

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

Example

The following example sets all interfaces as passive, then activates VLAN 100:

```
passive-interface default
no passive-interface vlan100
```

51.23 redistribute (OSPFv3)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

Syntax

redistribute *source-protocol* [*process-id*] [**include-connected**] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected**] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**route-map** *map-tag*]

Parameters

- **source-protocol**—Source protocol from which routes are being redistributed. It can be one of the following keywords: **connected**, **static**, **ospf** or **bgp**.
- **process-id**—The *process-id* argument is used only together with the **ospf** keyword and specifies the appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. If it is omitted then a value of 1 is assumed.
- **include-connected**—Allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
- **metric** *metric-value*—Specifies the metric assigned to the redistributed routes.

- If the metric value is set by the route map (by the **set metric** command) then the value will supersede the metric value specified by the *metric-value* argument.

If no metric is specified, the following metric is assigned depending on the source protocol:

o from OSPF

a. the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process.

b. the external OSPF metric from the redistribution source process is advertised as the external metric with value of 1.

o from BGP - 1

o from any protocol except OSPF and BGP - 20

- **metric-type** *type-value*—Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:
  - **1**—Type 1 external route
  - **2**—Type 2 external route

If a **metric-type** is not specified, a Type 2 external route is adopted.

- **match** {**internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}—The **match** keyword is used only together with the **ospf** keyword and specifies the criteria by which OSPF routes are redistributed into the target OSPF process. It can be one of the following:
  - **internal**- Routes that are internal to a specific autonomous system.
  - **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route.
  - **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.
  - **nssa-external 1**—Routes that are external to the autonomous system but are imported into OSPF, in a not so stubby area (NSSA), for IPv6 as Type 1 external routes.
  - **nssa-external 2**—Routes that are external to the autonomous system but are imported into OSPF, in a not so stubby area (NSSA), for IPv6 as Type 2 external routes.

By default the **internal** and **external 1** routes are redistributed.

Note. A few the **redistribute** commands with different values of the **match** keyword may be defined.

route-map—Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If the route-map keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.

map-tag—Identifier of a configured route map.

Default Configuration

Route redistribution is disabled.

Command Mode

Address family configuration

Router configuration

User Guidelines

Routes distributed to the source protocol are never redistributed by it

The **connected** keyword is used to redistribute to the target OSPF autonomous system routes that correspond to defined IP interfaces on which the destination OSPF process is not enabled. By default, the OSPF process advertises only IP interfaces on which the OSPF process is enabled.

The **static** keyword is used to redistribute to the target OSPF process static routes. By default, static routes are not redistributed to OSPF.

The **bgp** keyword is used to redistribute from BGP to OSPF routes learned by eBGP. Routes learned by iBGP are redistributed only if it was configured by the **bgp redistribue-internal** command.

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting.

Note. In IPv4, if you redistribute a protocol, by default you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6 this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the **include-connected** keyword. In IPv6 this functionality is not supported when the source protocol is BGP.

Example

Example 1. The following example redistributes IS-IS for IPv6 routes into the OSPF for IPv6 routing process 1:

```
ipv6 router ospf 1
 redistribute isis 1 metric 32 metric-type 1 tag 85
exit
```

Example 2. In the following example, ospf 1 redistributes the prefixes 2001:1:1::/64 and 2001:99:1::/64 and any prefixes learned through rip 1:

```
interface vlan 100
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable
exit
interface vlan 101
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable
exit
interface vlan102
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1
 ipv6 router ospf 1
  redistribute rip 1 include-connected
 exit
exit
```

51.24 router-id (IPv6)

To use a fixed router ID, use the **router-id** command in router configuration mode. To return to the default, use the **no** form of this command.

Syntax

router-id {*ipv4-address* | *integer-value*}

no router-id

Parameters

- **ipv4-address**—Router ID in IPv4 address format.
- **integer-value**—Router ID as a positive integer value.

Default Configuration

The mini minimum IPv4 address configured on the router.

Command Mode

Router configuration

User Guidelines

You can configure an arbitrary value in the IP address or integer format for each router. However, each router ID must be unique.

When the router ID of an OSPF process is changed the OSPF process is automatical restarted (the same effect like from the **clear ipv6 ospf process** command)

If the router ID of an OSPF process is not defined and the switch does not have an IPv4 address the OSPF process operational state is down.

Example

The following example specifies a fixed router ID:

```
ipv6 router ospf 1
  router-id 10.1.1.1
exit
```

51.25 show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 ospf [*process-id* [*area-id*]]

Parameters

- **process-id**—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
- **area-id**—Area ID. This argument displays information about a specified area only.

Default Configuration

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Example

The following is sample output from the **show ipv6 ospf** command:

```
Router# show ip ospf

OSPFv3 Routing Process 1 with ID 192.168.0.0
 Administrative state is UP
 Operational state is UP
 Default Redistribute Metric is 100
 Redistributing is enabled from
  Connected:
   metric value is default metric
   metric type is external 2
   route-map name is alpha
   with subnets
   nssa only
  Connected:
   metric value is default metric
   metric type is external 2
   route-map name is alpha
   with subnets
   nssa only
  static:
   metric value is 50
   metric type is external 1
   no route-map
   without subnets
  OSPF 109:
   internal:
    internal  metric value is preserved, metric type is external 1
     metric value is preserved, metric type is external 1
     route-map name is alp
      with subnets
    exteranl 1
      metric value is 100, metric type is external 1
      no route-map
```

```
        with subnets
      exteranl 2
        metric is value 100, metric type is external 2
        no route-map
        with subnets
  OSPF 120:
    from metric type:
      internal:  metric value is default metric, metric type is external 1
        metric value is default metric, metric type is external 1
        no route-map
        with subnets
      exteranl 1: metric value is default metric, metric type is external 2
        metric value is default metric, metric type is external 2
        no route-map
        with subnets
It is an Autonomous System Boundary Router
It is an Area Boundary Router
SPF schedule delay 5000 ms
Maximum Number of Equal Cost Paths 4
Number of External LSAs (Type 5) is 6, Checksum is 0x11029BEB
Number of originated LSAs is 126
Number of received LSAs is 1006
Number of areas in this router is 4. 2 normal 1 stub 1 nssa
   Area BACKBONE(0)
       Administrative state is UP
       Operational state is UP
       Number of interfaces in this area is 2
       Area has message digest authentication
       SPF algorithm executed 4 times
       Area ranges are
          192.168.0.0/16 Advertise
          192.100.0.0/16 Not Advertise
       Number of ASBR is 0
       Number of ABR is 2
       Number of LSA 31. Checksum Sum 0x107493
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 20
   Area 24
       Administrative state is UP
       Operational state is UP
       Number of interfaces in this area is 2
       SPF algorithm executed 10 times
       Area ranges are
```

```
        Number of ASBR is 1
        Number of ABR is 3
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
    Area 10.0.0.0
        It is a NSSA area
        Administrative state is UP
        Operational state is UP
        Number of interfaces in this area is 4
        Area default metric is 100
        Perform type-7/type-5 LSA translation, suppress forwarding address
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
    Area 192.168.1.1
        It is a stub area, no summary
        Administrative state is UP
        Operational state is UP
        Number of interfaces in this area is 4
        Area default metric is 100
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
```

51.26 show ipv6 ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ipv6 ospf database** command in user EXEC or privileged EXEC mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

Syntax

show ipv6 ospf [*process-id* [*area-id*]] **database** [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**database-summary**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**external** [*ipv6-prefix*] [*link-state-id*]] | [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**grace**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**inter-area prefix** [*ipv6-prefix*] [*link-state-id*]] | [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**inter-area router** [*destination-router-id*] [*link-state-id*]] | [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**link** [**interface** *interface-name*] [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**network** [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**nssa-external** [*ipv6-prefix*] [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**prefix** [**ref-lsa** {**router** | **network**}] [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**router** [*link-state-id*]] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [[**router** | **network** | [**external** *ipv6-prefix* | **nssa-external** *ipv6-prefix* | **inter-area** {**prefix** *ipv6-prefix* | **router**}] | **link** | **prefix**] | **database-summary**] [**adv-router** *router-id* | **self-originate**] [**internal**]

show ipv6 ospf [*process-id* [*area-id*]] **database** [**unknown** [{**area** | **as** | **link**} [*link-state-id*]]] [**adv-router** *router-id* | **self-originate**] [**internal**]

Parameters

- **process-id**— Displays information only about a specified process.
- **area-id**— Displays information only about a specified area. The area-id argument can only be used if the process-id argument is specified.
- **adv-router** *router-id*—Displays all the LSAs of the advertising router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons.
- **self-originate**—Displays only self-originated LSAs (from the local router).
- **internal**—Internal LSA information.
- **database-summary**—Displays how many of each type of LSAs exist for each area in the database, and the total.
- **external**—Displays information only about the external LSAs.
- **ipv6-prefix**—Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
- **link-state-id**—An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
- **inter-area prefix**—Displays information only about LSAs based on inter-area prefix LSAs.
- **inter-area** *router*—Displays information only about LSAs based on inter-area router LSAs.
- **destination-router-id**— The specified destination router ID.
- **link**—Displays information about the link LSAs.
- **interface**— Displays information about the LSAs filtered by interface context.
- **interface-name**—Specifies the LSA interface.
- **network**—Displays information only about the network LSAs.
- **nssa-external**—Displays information only about the not so stubby area (NSSA) external LSAs.
- **prefix**—Displays information on the intra-area-prefix LSAs.
- **ref-lsa {router | network}**—Further filters the prefix LSA type.
- **router**—Displays information only about the router LSAs.
- **unknown**—Displays all LSAs with unknown types.
- **area**—Filters unknown area LSAs.
- **as**—Filters unknown autonomous system (AS) LSAs.
- **link**—When following the unknown keyword, the link keyword filters link-scope LSAs.

Default Configuration

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **adv-route**r keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf database** command to provide more detailed information.

Example

Example 1. The following is sample output from the show ipv6 ospf database command when no arguments or keywords are used:

```
show ipv6 ospf database

OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

        Router Link States (Area 0)
ADV Router             Age    Seq#          Fragment ID  Link count  Bits
172.16.4.4             239    0x80000003              0           1 B
172.16.6.6             239    0x80000003              0           1 B

        Inter Area Prefix Link States (Area 0)

ADV Router             Age    Seq#         Prefix
172.16.4.4             249   0x80000001  FEC0:3344::/32
172.16.4.4             219   0x80000001  FEC0:3366::/32
172.16.6.6             247   0x80000001  FEC0:3366::/32
172.16.6.6            193    0x80000001  FEC0:3344::/32
172.16.6.6              82   0x80000001  FEC0::/32

        Inter Area Router Link States (Area 0)
ADV Router             Age    Seq#         Link ID     Dest RtrID
172.16.4.4             219   0x80000001 50529027  172.16.3.3
172.16.6.6             193   0x80000001 50529027  172.16.3.3

        Link (Type-8) Link States (Area 0)
ADV Router             Age    Seq#         Link ID Interface
172.16.4.4            242    0x80000002  14       VLAN 100
172.16.6.6            252     0x80000002 14       VLAN 100

        Intra Area Prefix Link States (Area 0)
ADV Router             Age    Seq#         Link ID Ref-lstype  Ref-LSID
172.16.4.4             242    0x80000002 0        0x2001      0
172.16.6.6             252    0x80000002 0        0x2001      0
```

The description of thesignificant fields shown in the display.

ADV Router—Advertising router ID.

Age—Link-state age.

Seq#—Link-state sequence number (detects old or duplicate LSAs).

Link ID—Interface ID number.

Ref-lstype—Referenced link-state type.

Ref-LSID—Referenced link-state ID.

Example 2. The following is sample output from the show ipv6 ospf database command with the router self-originate keywords:

```
show ipv6 ospf database router self-originate

          OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

          Router Link States (Area 0)

LS age: 383
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000003
Checksum: 0x7543
Length: 40
Area Border Router
Number of Links: 1
  Link connected to: another Router (point-to-point)
  Link Metric: 1
  Local Interface ID: 14
  Neighbor Interface ID: 14
  Neighbor Router ID: 172.16.4.4
```

Example 3. The following is sample output from the show ipv6 ospf database command with the network keyword:

```
show ipv6 ospf database network

          OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

          Net Link States (Area 1)

LS age: 419
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Network Links
Link State ID: 3 (Interface ID of Designated Router)
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
```

```
Checksum: 0x8148
Length: 32
  Attached Router: 172.16.6.6
  Attached Router: 172.16.3.3
```

Example 4. The following is sample output from the show ipv6 ospf database command with the link self-originate keywords:

```
show ipv6 ospf database link self-originate

                OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

                Link (Type-8) Link States (Area 0)

LS age: 505
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Link-LSA (Interface: POS4/0)
Link State ID: 14 (Interface ID)
Advertising Router: 172.16.6.6
LS Seq Number: 80000002
Checksum: 0xABF6
Length: 60
Router Priority: 1
Link Local Address: FE80::205:5FFF:FED3:6408
Number of Prefixes: 2
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None
```

Example 5. The following is sample output from the show ipv6 ospf database command with the prefix self-originate keywords:

```
show ipv6 ospf database prefix self-originate

                OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

                Intra Area Prefix Link States (Area 0)

Routing Bit Set on this LSA
LS age: 552
LS Type: Intra-Area-Prefix-LSA
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000002
Checksum: 0xA910
Length: 48
Referenced LSA Type: 2001
Referenced Link State ID: 0
Referenced Advertising Router: 172.16.6.6
```

```
Number of Prefixes: 2
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None, Metric: 1
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None, Metric: 1
```

Example 6. The :following is sample output from the show ipv6 ospf database command with the inter-area prefix self-originate keywords

```
show ipv6 ospf database inter-area prefix self-originate

        OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

        Inter Area Prefix Link States (Area 0)

LS age: 587
LS Type: Inter Area Prefix Links
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x1395
Length: 32
Metric: 1
Prefix Address: FEC0:3366::
Prefix Length: 32, Options: None

LS age: 532
LS Type: Inter Area Prefix Links
Link State ID: 1
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x3197
Length: 32
Metric: 2
Prefix Address: FEC0:3344::
Prefix Length: 32, Options: None

LS age: 422
LS Type: Inter Area Prefix Links
Link State ID: 2
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0xCB74
Length: 32
Metric: 1
Prefix Address: FEC0::
Prefix Length: 32, Options: None
```

Example 7. The following is sample output from the show ipv6 ospf database command with the inter-area router self-originate keywords:

```
show ipv6 ospf database inter-area router self-originate

        OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

        Inter Area Router Link States (Area 0)

LS age: 578
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Inter Area Router Links
Link State ID: 50529027
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x369F
Length: 32
Metric: 1
Destination Router ID: 172.16.3.3
```

Example 8. The following is sample output from the show ipv6 ospf database command with the external keyword:

```
show ipv6 ospf database external

        OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

        Type-5 AS External Link States

Routing Bit Set on this LSA
LS age: 654
LS Type: AS External Link
Link State ID: 0
Advertising Router: 172.16.3.3
LS Seq Number: 80000001
Checksum: 0x218D
Length: 32
Prefix Address: FEC0:3333::
Prefix Length: 32, Options: None
Metric Type: 2 (Larger than any link state path)
Metric: 20
```

Example 9. The The following is sample output from the show ipv6 ospf database command for a graceful-restart-capable router:

```
show ipv6 ospf 1 database

        OSPFv3 Router with ID (10.2.2.2) (Process ID 1)

        Router Link States (Area 0)
```

```
ADV Router            Age    Seq#          Fragment ID Link count Bits
10.1.1.1             1949    0x8000000e  0              1          None
10.2.2.2              2007    0x80000011  0              1          None

            Link (Type-8) Link States (Area 0)
ADV Router            Age    Seq#          Link ID Interface
10.1.1.1              180    0x80000006  1        VLAN 100
10.2.2.2             2007    0x80000006  1        VLAN 100

            Intra Area Prefix Link States (Area 0)
ADV Router Age Seq# Link ID Ref-lstype Ref-LSID
ADV Router            Age    Seq#         Link ID  Ref-lstype  Ref-LSID
10.1.1.1              180    0x80000006  0         0x2001      0
10.2.2.2             2007   0x80000006   0         0x2001      0

            Grace (Type-11) Link States (Area 0)
ADV Router            Age    Seq#         Link ID  Interface
10.2.2.2             2007   0x80000005  1          VLAN 100
```

Example 10. The following is sample outpet from the show ipv6 ospf database command with the grace keyword:

```
show ipv6 ospf database grace

OSPFv3 Router with ID (10.3.33.3) (Process ID 1)

Grace (Type-11) Link States (Area 0)

  LS age: 2
  LS Type: Grace Links (Interface: Ethernet0/0)
  Link State ID: 3 (Interface ID)
  Advertising Router: 10.2.2.2
  LS Seq Number: 80000001
  Checksum: 0xE3DD
  Length: 36
  Grace Period : 120
  Graceful Restart Reason : Software reload/upgrade
```

The description of thesignificant fields shown in the display.

Grace (Type-11)—Type 11 indicates that this router is graceful-restart capable.

LS Type: Grace Links (Interfece: VLAN 100)—The link state type and interface used.

Grace Period : 120—The graceful-restart interval, in seconds.

Graceful Restart Reason: Software reload/upgrade—The reason graceful restart was activated.

51.27 show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **show ipv6 ospf interface** command in user EXEC or privileged mode.

Syntax

show ip ospf [*process-id* [*area-id*]] **interface** [*interface-id*] [**brief**]

Parameters

- **process-id**—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
- **area-id**—Displays information about a specified area only.
- **interface-id**—Interface identifier.
- **brief**—Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Default Configuration

Command Mode

Privileged EXEC

EXEC

User Guidelines

Example

Example 1. The following is sample output from the show ipv6 ospf interface command:

```
show ipv6 ospf interface

tunnel 1 is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Adminastrative state is up, Operational state is up
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
VLAN 100 is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Adminastrative state is up, Operational state is up
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6 (Designated Router)
  Suppress hello for 0 neighbor(s
```

The description of thesignificant fields shown in the display.

tunnel 1, vlan 100—Status of the network interface.

Link Local Address—Interface IPv6 address.

Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3—The area ID, process ID, instance ID, and router ID of the area from which this route is learned.

Network Type POINT_TO_POINT, Cost: 1—Network type and link-state cost.

Transmit Delay—Transmit delay, interface state, and router priority.

Designated Router—Designated router ID and respective interface IP address.

Backup Designated router—Backup designated router ID and respective interface IP address.

Timer intervals configured—Configuration of timer intervals.

Hello—Number of seconds until the next hello packet is sent out this interface.

Neighbor Count—Count of network neighbors and list of adjacent neighbors.

Example 2. The following sample output from the **show ipv6 ospf interface brief** command shows a summary of information:

```
Router# show ipv6 ospf interface brief

Interface        Process ID     Area ID          Cost    OSPF Oper St  Passive
-----------------  -------------    ---------------------   --------  -------------------  -----------
tunnel 2            1            172.116.211.116    100   up                 Yes
VLAN 1000           1            1.1.2.1                35  down
VLAN 1              1             20                    55   up
```

51.28 show ipv6 ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in user EXEC or privileged EXEC mode.

Syntax

show ip ospf [*process-id* [*area-id*]] **neighbor** [*interface-id*] [*neighbor-id*] [**detail**]

Parameters

- **process-id**—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
- **area-id**—Displays information only about a specified area.
- **interface-id**—Interface identifier.
- **neighbor-id**—Neighbor ID.
- **detail**—Displays all neighbors in detail (lists all neighbors).

Default Configuration

Command Mode

Privileged EXEC

EXEC

User Guidelines

Example

Example 1. The following is sample output from the show ipv6 ospf neighbor command:

```
show ipv6 ospf neighbor

Neighbor ID        Pri   State          Dead Time    Interface ID     Interface
172.16.4.4          1    FULL/ -        00:00:31     14               POS4/0
172.16.3.3          1    FULL/BDR       00:00:30     3                FastEthernet00
172.16.5.5          1    FULL/ -        00:00:33     13               ATM3/0
```

Example 2. The following is sample output from the show ipv6 ospf neighbor command with the **detail** keyword:

```
show ipv6 ospf neighbor detail

Neighbor 172.16.4.4
  In the area 0 via interface POS4/0
  Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
  Neighbor priority is 1, State is FULL, 6 state changes
  Options is 0x63AD1B0D
  Dead timer due in 00:00:33
  Neighbor is up for 00:48:56
Neighbor 172.16.3.3
  In the area 1 via interface FastEthernet0/0
  Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 172.16.6.6 BDR is 172.16.3.3
  Options is 0x63F813E9
  Dead timer due in 00:00:33
  Neighbor is up for 00:09:00
Neighbor 172.16.5.5
```

```
  In the area 2 via interface ATM3/0
  Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
  Neighbor priority is 1, State is FULL, 6 state changes
  Options is 0x63F7D249
  Dead timer due in 00:00:38
  Neighbor is up for 00:10:01
```

The description of thesignificant fields shown in the display.

Neighbor ID; Neighbor—Neighbor router ID.

In the area—Area and interface through which the OSPF neighbor is known.

Pri; Neighbor priority—Router priority of the neighbor, neighbor state.

State—OSPF state.

State changes—Number of state changes since the neighbor was created.

Options—Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)

Dead timer due in—Expected time before Cisco IOS software will declare the neighbor dead.

Neighbor is up for—Number of hours:minutes:seconds since the neighbor went into two-way state.

Example 3. The following is sample output from the show ipv6 ospf neighbor command with the detail keyword, displaying graceful-restart information:

```
show ipv6 ospf neighbor detail

Neighbor 10.1.1.1
  In the area 0 via interface Ethernet0/0
  Neighbor: interface-id 3, link-local address FE80::A8BB:CCFF:FE00:200
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.1.1.1 BDR is 10.3.3.3
  Options is 0x1C9AD11
  Dead timer due in 00:00:36
  Neighbor is up for 00:00:16
```

51.29 show ipv6 ospf router-id

To display OSPF process router-id, use the **show ipv6 ospf router-id** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 ospf [*process-id*] **router-id**

Parameters

process-id—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Default Configuration

N/A

Command Mode

Privileged EXEC

EXEC

User Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Example

The following is sample output from the **show ipv6 ospf router-id** command:

```
show ipv6 ospf router-id

Process-ID      Current Router-ID        Next Router-ID after Restart
                 Value            Type     Value            Type
--------------   -------------------   ---------   -------------------   ---------
           1    1.1.1.192         default  1.1.1.1           default
           2    1.1.1.192         default  100.100.100.100  manual
           3    2.2.2.2           manual  2.2.2.2           default
           4    10.10.10.10       manual  1.1.1.1           default
           5    10.10.10.10       manual   2.2.2.2          manual
```

51.30 show ipv6 ospf snmp

To display OSPF snmp configuration, use the **show ipv6 ospf snmp** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 ospf snmp

Command Mode

Privileged EXEC

EXEC

User Guidelines

Use the **show ipv6 ospf snmp** command to display the OSPF snmp configuration.

Example

The following is sample output from the **show ip ospf snmp** command:

```
show ip ospf snmp

The standard OSPF MIB is mapped to OSPF process 2
SNMP notifications for OSPF are enabled
SNMP notifications Rate Limit: 10 seconds and 7 notifications during the window time
```

```
Authentication Failure Notifications are enabled
Bad Packet Notifications are disabled
Configuration Error Notifications are enabled
Virtual Link Authentication-failure Notifications are disabled
Virtual Link Bad Packet Notifications are enabled
Virtual Link Configuration Error Notifications are enabled
SNMP LSA Notifications are disabled
SNMP Packet Retransmission Notifications are disabled
SNMP Virtual Packet Retransmission Notifications are disabled
SNMP IF State Change Notifications are enabled
SNMP Neighbor State Change Notifications are enabled
SNMP Virtual IF State Change Notifications are enabled
SNMP Virtual Neighbor State Change Notifications are enabled
```

51.31 show ipv6 ospf virtual-link

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 ospf virtual-links

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC

EXEC

User Guidelines

The information displayed by the show ipv6 ospf virtual-links command is useful in debugging OSPF routing operations.

Example

Example 1. The following is sample output from the show ipv6 ospf virtual-links command:

```
show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

The description of thesignificant fields shown in the display.

Virtual Link OSPF_VL0 to router 172.16.6.6 is up—Specifies the OSPF neighbor, and if the link to that neighbor is up or down.

Interface ID—Interface ID and IPv6 address of the router.

Transit area 2—The transit area through which the virtual link is formed.

via interface ATM3/0—The interface through which the virtual link is formed.

Cost of using 1—The cost of reaching the OSPF neighbor through the virtual link.

Transmit Delay is 1 sec—The transmit delay (in seconds) on the virtual link.

State POINT_TO_POINT—The state of the OSPF neighbor.

Timer intervals...—The various timer intervals configured for the link.

Hello due in 0:00:06—When the next hello is expected from the neighbor.

Example 2. The following sample output from the show ipv6 ospf virtual-links command has two virtual links:

```
show ipv6 ospf virtual-links

Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
  Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial12/0, Cost of using 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
    Adjacency State FULL (Hello suppressed)
    Index 1/2/4, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
  Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial11/0, Cost of using 128
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Adjacency State FULL (Hello suppressed)
```

51.32 shutdown (IPv6 OSPF)

To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the **shutdown** command in router configuration mode. To restart the OSPF protocol, use the **no** form of this command.

Syntax

shutdown

no shutdown

Parameters

N/A

Default Configuration

OSPF stays active under the current instance.

Command Mode

Router configuration (config-router)

User Guidelines

Use the **shutdown** command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.

The **no shutdown** command changes the OSPF process router-id if it was reconfigured by the user else if the current used router-id has the default value the command runs the router-id re-election algorithm.

Example

The following example shows how to enable a graceful shutdown of the OSPF protocol:

```
ipv6 router ospf 1
  shutdown
exit
```

51.33 snmp-process ipv6 ospf

To specify an OSPF process accessed via the standard OSPF MIB, use the **snmp-process ipv6 ospf** command in global configuration mode. To return to the default, use the **no** form of this command.

Syntax

snmp-process ipv6 ospf *process-id*

no snmp-process ipv6 ospf [*process-id*]

Parameters

process-id—OSPF process ID.

Default Configuration

The minimal existed OSPF process.

Command Mode

Global configuration mode

User Guidelines

The standard MIB do not include the OSPF process-ID and by default is mapped to the minimal OSPF process. Use the **snmp-process ipv6** command to change the mapping.

Example

The following example maps the standard MIBs to OSPF process 100:

```
snmp-process ipv6 ospf 100
```

51.34 snmp-server enable traps ipv6 ospf

To enable all Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF), use the **snmp-server enable traps ipv6 ospf** command in global configuration mode. To disable all SNMP notifications for OSPF, use the **no** form of this command.

Syntax

snmp-server enable traps ipv6 ospf

no snmp-server enable traps ipv6 ospf

Parameters

N/A

Default Configuration

SNMP notifications for OSPF are disabled.

Command Mode

Global configuration

User Guidelines

If you wish to enable or disable specific OSPF SNMP notifications, enter one or more of the following commands of the following commands:

[**no**] **snmp-server enable traps ipv6 ospf errors**

[**no**] **snmp-server enable traps ipv6 ospf lsa**

[**no**] **snmp-server enable traps ipv6 ospf retransmit**

[**no**] **snmp-server enable traps ipv6 ospf state-change**

Example

The following exampleglobally enables SNMP notifications for OSPF:

```
Router(config)# snmp-server enable traps ipv6 ospf
```

51.35 snmp-server enable traps ipv6 ospf errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) errors, use the s**nmp-server enable traps ipv6 ospf errors** command in global configuration mode. To disable SNMP notifications for OSPF errors, use the **no** form of this command.

Syntax

snmp-server enable traps ipv6 ospf errors [**authentication-failure**][**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

no snmp-server enable traps ipv6 ospf errors [**authentication-failure**][**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

Parameters

- **authentication-failure**—Enables only the ospfIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a nonvirtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
- **bad-packet**—Enables only the ospfIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a nonvirtual interface.
- **config-error**—Enables only the ospfIfConfigError trap. Sends SNMP notifications when a packet has been received in a nonvirtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.
- v**irt-authentication-failure**—Enables only the ospfVirtIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a virtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
- **virt-bad-packet**—Enables only the ospfVirtIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a virtual interface.
- **virt-config-error**—Enables only the ospfVirtIfConfigError trap. Sends SNMP notifications when a packet has been received in a virtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

Default Configuration

SNMP notifications for OSPF errors are disabled.

Command Mode

Global configuration

User Guidelines

When you enter the **snmp-server enable traps ipv6 ospf errors** command without any optional keywords, all OSPF error traps will be enabled. To enable only one or more OSPF error traps, enter one or more of the optional keywords.

Example

The following example enables the router to send all OSPF error notifications:

```
Router(config)# snmp-server enable traps ipv6 ospf errors
```

51.36 snmp-server enable traps ipv6 ospf lsa

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) link-state advertisements (LSAs), use the **snmp-server enable traps ipv6 ospf lsa** command in global configuration mode. To disable SNMP notifications for OSPF LSAs, use the **no** form of this command.

Syntax

snmp-server enable traps ipv6 ospf lsa [**lsa-maxage**] [**lsa-originate**]

no snmp-server enable traps ipv6 ospf lsa [**lsa-maxage**] [**lsa-originate**]

Default Configuration

SNMP notifications for OSPF LSAs are disabled.

Command Mode

Global configuration

User Guidelines

The **snmp-server enable traps ipv6 ospf lsa** command enables the traps for standard LSAs that are defined by the OSPF-MIB. To enable the ospfMaxAgeLsa trap, enter the **snmp-server enable traps ipv6 ospf lsa** command with the **lsa-maxage** keyword. To enable the ospfOriginateLsa trap, enter the **snmp-server enable traps ipv6 ospf lsa** command with the **lsa-originate** keyword. When the ospfOriginateLsa trap is enabled, it will not be invoked for simple LSA refreshes that take place every 30 minutes or when an LSA has reached its maximum age and is being flushed. When you enter the **snmp-server enable traps ipv6 ospf lsa** command without either keyword, both traps will be enabled.

To enable the traps that are defined by the CISCO-OSPF-TRAP-MIB for opaque LSAs, enter the **snmp-server enable traps ipv6 ospf cisco-specific lsa** command in global configuration mode.

Example

The following example enables the router to send SNMP notifications when new LSAs are originated by the router as a result of a topology change:

```
Router(config)# snmp-server enable traps ipv6 ospf lsa lsa-originate
```

51.37 snmp-server enable traps ipv6 ospf rate-limit

To limit the number of Open Shortest Path First (OSPF) traps that are sent during a specified number of seconds, use the **snmp-server enable traps ipv6 ospf rate-limit** command in global configuration mode. To disable the limit placed on the number of OSPF traps sent during a specified number of seconds, use the **no** form of this command.

Syntax

snmp-server enable traps ipv6 ospf rate-limit *seconds trap-number*

no snmp-server enable traps ipv6 ospf rate-limit *seconds trap-number*

Parameters

- **seconds**—Sets the rate limit window size, in seconds. A number from 2 to 60. The default value is 10.
- **trap-number**—Sets the maximum number of traps sent during the window time. A number from 0 to 300. The default number is 7.

Default Configuration

No limit is placed on the number of OSPF traps sent.

Command Mode

Global configuration

User Guidelines

There is a possibility that a router sends trap bursts, which can drain network resources in a small interval of time. It is recommended that you enter the **snmp-server enable traps ipv6 ospf rate-limit** command to configure a sliding window mechanism that will limit the number of traps that are sent within a specified number of seconds

Example

he following example sets the trap rate limit window so that during a 40-second window of time, no more that 50 traps are sent:

```
Router(config)# snmp-server enable traps ipv6 ospf rate-limit 40 50
```

51.38 snmp-server enable traps ipv6 ospf retransmit

To enable Simple Network Management Protocol (SNMP) notifications when packets are re-sent in an Open Shortest Path First (OSPF) network, use the **snmp-server enable traps ipv6 ospf retransmit** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

Syntax

snmp-server enable traps ipv6 ospf retransmit [**packets**] [**virt-packets**]

no snmp-server enable traps ipv6 ospf retransmit [**packets**] [**virt-packets**]

Parameters

- **packets**—Enables only the ospfTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a nonvirtual interface.
- **virt-packets**—Enables only the ospfVirtTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a virtual interface.

Default Configuration

SNMP notifications are disabled.

Command Mode

Global configuration

User Guidelines

To enable the ospfTXRetransmit trap so that SNMP notifications are sent only when packets from nonvirtual interfaces are re-sent, enter the **snmp-server enable traps ipv6 ospf retransmit** command with the **packets** keyword. To enable the ospfTxRetransmit trap so that SNMP notifications are sent only when packets from virtual interfaces are re-sent, enter the **snmp-server enable traps ipv6 ospf retransmit** command with the **virt-packets** keyword. When you enter the **snmp-server enable traps ipv6 ospf retransmit** command without either keyword, both traps will be enabled.

Example

The following example enables the router to send SNMP notifications when packets are re-sent by virtual interfaces:

```
Router(config)# snmp-server enable traps ipv6 ospf retransmit virt-packets
```

51.39 snmp-server enable traps ipv6 ospf state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ipv6 ospf state-change** command in global configuration mode. To disable SNMP notifications for OSPF transition state changes, use the **no** form of this command.

Syntax

snmp-server enable traps ipv6 ospf state-change [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

no snmp-server enable traps ipv6 ospf state-change [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

Parameters

- **if-state-change**—Enables only the ospfIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF interface.
- **neighbor-state-change**—Enables only the ospfNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF neighbor.
- **virtif-state-change**—Enables only the ospfVirtIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF interface.
- **virtneighbor-state-change**—Enables only the ospfVirtNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF neighbor.

Default Configuration

SNMP notifications for OSPF transition state changes are disabled.

Command Mode

Global configuration

User Guidelines

To enable all traps for transition state changes, enter the **snmp-server enable traps ipv6 ospf state-chang**e command without of the optional keywords.

Example

The following example enables the router to send SNMP notifications for transition state changes for virtual interfaces and virtual neighbors:

```
Router(config)# snmp-server enable traps ipv6 ospf state-change virtif-state-change
virtneighbor-state-change
```

52 Open Shortest Path First (OSPF) Commands

52.1 area filter-list

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the **area filter-list** command in router configuration mode. To cancel the filter, use the **no** form of this command.

Syntax

area *area-id* **filter-list prefix** *prefix-list-name* {**in** | **out**}

no area *area-id* **filter-list prefix** {**in** | **out**}

Parameters

- **area-id**—Identifier of the area for which filtering is configured. The identifier can be specified as either a decimal value or an IP address.
- **prefix-list-name**—Name of a prefix list.
- **in**—The prefix list is applied to prefixes advertised to the specified area from other areas.
- **out**—The prefix list is applied to prefixes advertised out of the specified area to other areas.

Default Configuration

This command is disabled by default. The router will not filter prefixes.

Command Mode

Router configuration (config-router)

User Guidelines

If the area does not exist when the **area filter-list** command is applied it is created.

The **area filter-list** command impacts only on an ABR. If the **area filter-list** command is configured on non ABR the configuration is saved but it is not applied.

With this feature enabled in the "**in**" direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the **area range** command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.

With this feature enabled in the "**out**" direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the **area range** command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if at least one prefix in the area range matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the **area range** command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

Example

The following example filters prefixes that are sent from all other areas to area 1:

```
area 1 filter-list prefix AREA_1 in
```

52.2 clear ip ospf process

To restart the Open Shortest Path First (OSPF) process, use the **clear ip ospf process** command in privileged EXEC mode.

Syntax

clear ip ospf [*process-id*] **process**

Parameters

process-id—Process ID. If the parameter is omitted all the OSPF processes are restarted.

Default Configuration

N/A

Command Mode

Privileged EXEC

User Guidelines

Use the *process-id* argument to restart only one OSPF process. If the *process-id* argument is not specified, all OSPF processes are restarted.

The **clear ip ospf process** command changes the OSPF process router-id if it was reconfigured by the user else if the current used router-id has the default value the command runs the router-id re-election algorithm.

Example

Example 1. The following example restarts all the OSP processes:

```
clear ip ospf process
```

Example 2. The following example restarts one OSP process with process-id 1:

```
clear ip ospf 1 process
```

52.3 ip ospf authentication

To override the area default authentication type for an IP interface, use the **ip ospf authentication** command in IP interface configuration mode. To return to the area default authentication type for an interface, use the **no** form of this command.

Syntax

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Parameters

- **message-digest**—Specifies that MD5 authentication will be used.
- **null**—No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.

Default Configuration

The area default authentication type.

Command Mode

IP Interface configuration

User Guidelines

Specifying default authentication for an area without keyword sets the authentication to Type 1 (simple password) as specified in RFC 2328, Appendix D. If this command is not included in the configuration file, the area default authentication of type is assumed.

If you enable the MD5 authentication, you must configure a key chain name with the **ip ospf authentication key-chain** interface command. If a key chain is not defined for the IP interface or there is not a valid key then RIP packets are not sent on the IP interface and received IP interface packets are dropped.

If you enable the simple password authentication, you must configure a password with the **ip ospf authentication-key** interface command. If a password is not defined for the IP interface then OSPF packets are not sent on the IP interface and received IP interface packets are dropped.

Example

The following example overides the area default authentication for the `10.56.0.201`and 10.10.1.1 IP interfaces:

```
router ospf
 area 10.0.0.0 authentication
 network 10.56.0.201 area 10.0.0.0
 network 10.10.1.1 area 10.0.0.0
 network 10.2.1.1 area 10.0.0.0
exit
interface ip 10.56.0.201
 ip ospf authentication message-digest
 ip ospf authentication key-chain chain2
exit
interface ip 10.10.1.1
 ip ospf authentication null
exit
interface ip 10.2.1.1
 ip ospf authentication-key Ases12@@@#$4
exit
```

52.4 ip ospf authentication key-chain

To define a name of key chain to be used by authentication, use the **ip ospf authentication key-chain** command in IP interface configuration mode. To return to default, use the **no** form of this command.

Syntax

ip ospf authentication key-chain *name-of-chain*

no ip ospf authentication key-chain

Parameters

name-of-chain—Specifies the name of key chain.

Default Configuration

No key chain is specified.

Command Mode

IP Interface configuration

User Guidelines

Use the **ip ospf authentication key-chain** IP Interface Configuration mode command to define a key chain name. Only one key chaine may be defined per an IP interface. Each the **ip ospf authentication key-chain** command overides the previous definition.

Example

The following example defines chain1 and chain2:

```
router ospf
 area 10.0.0.0 authentication
 area 0 authentication
 network 10.56.0.201 area 10.0.0.0
 network 192.168.251.201 area 0
exit
interface ip 192.168.251.201
 ip ospf authentication key-chain chain1
exit
interface ip 10.56.0.201
 ip ospf authentication key-chain chain2
exit
```

52.5 ip ospf authentication-key

To assign a password to be used by neighboring routers that are using the OSPF simple password authentication, use the **ip ospf authentication-key** command in IP interface configuration mode. To remove a previously assigned OSPF password, use the **no** form of this command.

Syntax

ip ospf authentication-key *password*

no ip ospf authentication-key

Parameters

password—Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.

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 OSPF header when the switch software originates 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 OSPF information.

Only one password may be defined per an IP interface. Each the **ip ospf authentication-key** command overides the previous definition.

Example

The following example shows how to define a password:

```
interface ip 1.1.1.1
  ip ospf authentication mode text
  ip ospf authentication-key alpha$$1267
exit
```

52.6 ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** command in IP interface configuration mode. To reset the path cost to the default value, use the **no** form of this command.

Syntax

ip ospf cost *interface-cost*

no ip ospf cost

Parameters

interface-cost—Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.

Default Configuration

The default value depends on the interface’s ifSpeed (see **User Guidelines**).

Command Mode

IP Interface configuration

User Guidelines

You must define OSPF on an IP interface by the **network** command before using of the **ip ospf cost** command on the same IP interface.

You can set the metric manually using this command, if you need to change the default.

In general, the path cost is calculated using the following formula:

10^10 / ifSpeed

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

10G Ethernet Default cost is 1

1G Ethernet Default cost is 10

100M Ethernet Default cost is 100

10M Ethernet Default cost is 1000

Example

The following example sets the interface cost value to 65:

```
ip ospf cost 65
```

52.7 ip ospf dead-interval

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the **ip ospf dead-interval** command in IP interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Parameters

seconds—Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network.

Default Configuration

Four times the interval set by the **ip ospf hello-interval** command.

Command Mode

IP Interface configuration

User Guidelines

The dead interval is advertised in OSPF hello packets. This value must be the same for all networking devices on a specific network.

Example

The following example sets the OSPF dead interval to 20 seconds:

```
interface ip 1.1.1.1
 ip ospf dead-interval 20
exit
```

52.8 ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the IP interface, use the **ip ospf hello-interval** command in IP interface configuration mode. To return to the default time, use the **no** form of this command.

Syntax

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameters

seconds—Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. The range is from 1 to 65535.

Default Configuration

10 seconds

Command Mode

IP Interface configuration

User Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Example

The following example sets the interval between hello packets to 15 seconds:

```
interface ip 1.1.1.1
 ip ospf hello-interval 15
exit
```

52.9 ip ospf mtu-ignore

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (DBD) packets, use the **ip ospf mtu-ignore** command in IP interface configuration mode. To reset to default, use the **no** form of this command.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameters

N/A

Default Configuration

OSPF MTU mismatch detection is enabled.

Command Mode

IP Interface configuration

User Guidelines

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Example

The following example disables MTU mismatch detection on receiving DBD packets:

```
interface ip 1.1.1.1
 ip ospf mtu-ignore
exit
```

52.10 ip ospf passive-interface

To disable sending OSPF routing updates on an IP interface, use the **ip ospf passive-interface** command in IP interface configuration mode. To re-enable the sending of OSPF routing updates, use the **no** form of this command.

Syntax

ip ospf passive-interface

no ip ospf passive-interface

Parameters

N/A

Default Configuration

Routing updates are sent on the interface.

Command Mode

IP Interface configuration

User Guidelines

OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

Example

The following example sets all OSPF IP interfaces as passive and then activates Ethernet interface 0:

```
router ospf 100
  network 1.1.1.1 area 0
  passive-interface default
exit
```

```
interface ip 1.1.1.1
 no passive-interface
exit
```

52.11 ip ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ip ospf priority** command in IP interface configuration mode. To return to the default value, use the **no** form of this command.

Syntax

ip ospf priority *number-value*

no ip ospf priority

Parameters

number-value—A number value that specifies the priority of the router. The range is from 0 to 255.

Default Configuration

Priority of 1.

Command Mode

IP Interface configuration

User Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Example

The following example sets the router priority value to 4:

```
interface ip 1.1.1.1
 ip ospf priority 4
exit
```

52.12 ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the IP interface, use the **ip ospf retransmit-interval** command in IP interface configuration mode. To return to the default value, use the **no** form of this command.

Syntax

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Parameters

seconds—Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds. The default is 5 seconds.

Default Configuration

5 seconds.

Command Mode

IP Interface configuration

User Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of the *seconds* argument should be greater than the expected round-trip delay between any two routers on the attached network. The setting of this parameter should also be conservative, or needless LSA retransmissions may occur. The value should be larger for serial lines and virtual links.

Note. It is recommended to use the same value for the seconds argument on neighbor OSPF routers. Using inconsistent values on neighbor routers can cause needless LSA retransmissions.

Example

The following example sets the retransmit interval value to 8 seconds:

```
interface ip 1.1.1.1
 ip ospf retransmit-interval 8
exit
```

52.13 ip ospf shutdown

To initiate an Open Shortest Path First (OSPF) protocol graceful shutdown at the IP interface level, use the **ip ospf shutdown** command in interface configuration mode. To restart the OSPF protocol on an interface, use the **no** form of this command.

Syntax

ip ospf shutdown

no ip ospf shutdown

Parameters

N/A

Default Configuration

Command Mode

IP Interface configuration

User Guidelines

Use the **ip ospf shutdown** command to put OSPF on a specific interface in shutdown mode.

Example

The following example shows how to initiate an OSPF protocol shutdown on IP interface 1.1.1.1:

```
interface ip 1.1.1
  ip ospf shutdown
# exit
```

52.14 ip ospf transmit-delay

To set the estimated time required to send a link-state update packet on the IP interface, use the **ip ospf transmit-delay** command in IP interface configuration mode. To return to the default value, use the **no** form of this command.

Syntax

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Parameters

seconds—Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Default Configuration

1 second.

Command Mode

IP Interface configuration

User Guidelines

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Example

The following example sets the retransmit delay value to 3 seconds:

```
interface ip 1.1.1.1
 ip ospf transmit-delay 3
exit
```

52.15 network area

To define the IP interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for interfaces defined with the ip-address wildcard-mask pair, use the **no** form of this command.

Syntax

network *ip-address* **area** *area-id* [**shutdown**]

no network *ip-address*

Parameters

- **ip-address**—IP address.
- **area-id** —Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument.
- **shutdown**—OSPF is enabled on the interface in the shutdown state

Default Configuration

This command is disabled by default.

Command Mode

Router configuration (config-router)

User Guidelines

OSPF 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 **network** CLI command with the **shutdown** keyword to create OSPF on an interface if you are going to change the default values of RIP configuration and the use the **no ip ospf shutdown** CLI command.

Use the **no network** CLI command to remove OSPF on an IP interface and remove its interface configuration.

Note. Any individual IP interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the **network** command list and ignore the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap in order to avoid inadvertent conflicts.

Example

Example 1.The following example shows how to enable OSPF on IP interface 1.1.1.1 with the default interface configuration:

```
router ospf
 network 1.1.1.1 area 0
exit
```

Example 2. The following example enables OSPF on 1.1.1.1 in the shutdown state, configures the interface cost and starts OSPF:

```
router ospf
 network 1.1.1.1 area 0 shutdown
```

```
exit
interface ip 1.1.1.1
  ip ospf cost 102
  no ip ospf shutdown
exit
```

52.16 no area

To remove the specified area from the software configuration, use the **no area** command in router configuration mode.

Syntax

no area *area-id*

Parameters

area-id—Identifier for the removed area. The identifier can be specified as either a decimal value or an IP address.

Default Configuration

Area is defined.

Command Mode

Router configuration (config-router)

User Guidelines

To remove the specified area from the software configuration, use the **no area** *area-id* command. That is, the **no area** *area-id* command removes all area options, including **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Example

The following example removes area 1:

```
router ospf 1
 no area 1
exit
```

52.17 passive-interface (OSPF)

To disable sending OSPF routing updates on all OSPF IP interfaces, use the **passive-interface** command in router configuration mode. To re-enable the sending of OSPF routing updates, use the **no** form of this command.

Syntax

passive-interface

no passive-interface

Parameters

N/A

Default Configuration

Routing updates are sent on all OSPF IP interfaces.

Command Mode

Router configuration (config-router)

User Guidelines

OSPF routing information is neither sent nor received through all OSPF IP interfaces. A passive IP interface address appears as a stub network in the OSPF domain.

After using of the **passive-interface** command you can then configure individual interfaces where adjacencies are desired using the **no ip ospf passive-interface** command. The **passive-interface** command is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Example

The following example sets all OSPF IP interfaces as passive and then activates IP interface 1.1.1.1:

```
router ospf 100
  network 1.1.1.1 area 0
  passive-interface
exit
interface ip 1.1.1.1
 no ip ospf passive-interface
exit
```

52.18 redistribute (OSPF)

To redistribute routes from one routing domain into OSPF routing domain, use the **redistribute** command in the appropriate configuration mode. To disable redistribution, use the **no** form of this command.

Syntax

redistribute *protocol* [*process-id*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1**| **external 2**}] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

no redistribute *protocol* [*process-id*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1**| **external 2**}] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

Parameters

- **protocol**—Source protocol from which routes are being redistributed. It can be one of the following keywords: **connected**, **static**, **rip**, **ospf** or **bgp**.
- **process-id**—The *process-id* argument is used only together with the **ospf** keyword and specifies the appropriate OSPF process ID from which routes are to be redistributed. This

identifies the routing process. This value takes the form of a nonzero decimal number. If it is omitted then a value of 1 is assumed.

- **metric** *metric-value*—Specifies the metric assigned to the redistributed routes.

  If the metric value is set by the route map (by the **set metric** command) then the value will supersede the metric value specified by the *metric-value* argument.

  If no metric is specified, the following metric is assigned depending on the source protocol:

  - from OSPF

  a) The internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process.

  b) The external OSPF metric from the redistribution source process is advertised as the external metric with value of 1.

  - from BGP - 1
  - from any protocol except OSPF and BGP - 20

- **metric-type** *type-value*—Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:

  - **1** - Type 1 external route
  - **2** - Type 2 external route

  If a **metric-type** is not specified, a Type 2 external route is adopted.

- **match** {**internal** | **external 1** | **external 2**}—The **match** keyword is used only together with the **ospf** keyword and specifies the criteria by which OSPF routes are redistributed into the target OSPF process. It can be one of the following:

  - **internal** - Routes that are internal to a specific autonomous system.
  - **external 1** - Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route.
  - **external 2** - Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.

  By default the **internal** and **external 1** routes are redistributed.

  Note. A few the **redistribute** commands with different values of the **match** keyword may be defined.

- **route-map**—Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
- **map-tag**—Identifier of a configured route map.
- **subnets**—For redistributing routes into OSPF, the scope of redistribution for the specified protocol. If the **subnets** keyword is not specified, only routes that are not subnetted are redistributed. By default, no subnets are defined.
- **nssa-only**—Sets the nssa-only attribute for all routes redistributed into OSPF. On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to a NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Default Configuration

Route redistribution is disabled.

Command Mode

Router configuration (config-router)

User Guidelines

Routes distributed to the source protocol are never redistributed by it

The **connected** keyword is used to redistribute to the target OSPF autonomous system routes that correspond to defined IP interfaces on which the destination OSPF process is not enabled. By default, the OSPF process advertises only IP interfaces on which the OSPF process is enabled.

The **static** keyword is used to redistribute to the target OSPF process static routes. By default, static routes are not redistributed to OSPF.

The **bgp** keyword is used to redistribute from BGP to OSPF routes learned by eBGP. Routes learned by iBGP are redistributed only if it was configured by the **bgp redistribue-internal** command.

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting.

Example

Example 1. The following example causes RIP routes to be redistributed into an OSPF domain:

```
router ospf 110
  redistribute rip metric 200 subnets
exit
```

Example 2. The following example causes the specified RIP and BGP processes routes to be redistributed into an OSPF domain. The RIP-derived metric will be remapped to 100 and BGP routes to 200:

```
router ospf 109
  redistribute rip metric 100 metric-type 1 subnet
  redistribute bgp 100 metric 200 metric-type 2 subnet
exit
```

Example 3. In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
interface vlan 2 0
  ip address 172.16.0.1 255.0.0.0
exit
interface vlan 10
  ip address 10.0.0.1 255.0.0.0
exit
router ospf 2
```

```
  network 172.16.0.1 area 0
exit
interface ip 172.16.0.1
  ip ospf cost 100
exit
router ospf 1
  network 10.0.0.1 area 0
  redistribute ospf 2 subnet
exit
```

Example 4. In the following example, internal route are redistributed from OSPF process 1 to OSPF process 2 with their metrics as external 1; external 1 routes are redistributed with metric equal to 100 as external 1 and external 2 routes are redistributed with metric equal to 200 as external 2 :

```
router ospf 2
  redistribute ospf 1 match internal metric-type 1 subnet
  redistribute ospf 1 match external 1 metric-type 1 metric 100 subnet
  redistribute ospf 1 match external 2 metric-type 2 metric 200 subnet
exit
```

Example 5. The following example removes the subnets options:

```
no redistribute ospf subnets
```

Example 6. The following example removes the redistribute bgp command, and any of the options that were configured for the redistribute bgp command, from the configuration:

```
no redistribute bgp
```

52.19 router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

Syntax

router ospf [*process-id*]

no router ospf [*process-id*]

Parameters

process-id—Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. The default value is 1.

Default Configuration

No OSPF routing process is defined.

Command Mode

Global configuration

User Guidelines

The no format of the **router ospf** commnad removes the OSPF configuration.

Use the **TBD** command to disable OSPF without OSPF configuration removing.

Example

The following example configures an OSPF routing process:

```
Router(config)# router ospf 2
```

52.20 router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. To return to the default, use the **no** form of this command.

Syntax

router-id *ip-address*

no router-id *ip-address*

Parameters

ip-address—Router ID in IP address format.

Default Configuration

The minimum IPv4 address configured on the router.

Command Mode

Router configuration (config-router)

User Guidelines

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the **clear ip ospf process** command.

Example

The following example specifies a fixed router-id:

```
router ospf 1
 router-id 10.1.1.1
exit
```

52.21 show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in user EXEC or privileged EXEC mode.

Syntax

show ip ospf [*process-id*]

Parameters

process-id—Process ID. If this argument is included, only information for the specified routing process is included.

Command Mode

User EXEC

Privileged EXEC

Example The following is sample output from the **show ip ospf** command:

```
Router# show ip ospf

OSPF Routing Process 1 with ID 192.168.0.0
  Administrative state is UP
  Default Redistribute Metric is 100
  Redistributing is enabled from
    Connected:
      metric value is default metric
      metric type is external 2
      route-map name is alpha
      with subnets
      nssa only
    Connected:
      metric value is default metric
      metric type is external 2
      route-map name is alpha
      with subnets
      nssa only
   static:
      metric value is 50
      metric type is external 1
      no route-map
      without subnets
    OSPF 109:
      internal:
        internal  metric value is preserved, metric type is external 1
          metric value is preserved, metric type is external 1
      route-map name is alp
      with subnets
    exteranl 1
      metric value is 100, metric type is external 1
      no route-map
      with subnets
    exteranl 2
      metric is value 100, metric type is external 2
      no route-map
      with subnets
  OSPF 120:
   from metric type:
    internal:  metric value is default metric, metric type is external 1
      metric value is default metric, metric type is external 1
      no route-map
      with subnets
    exteranl 1: metric value is default metric, metric type is external 2
      metric value is default metric, metric type is external 2
      no route-map
      with subnets
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an Autonomous System Boundary Router
It is an Area Boundary Router
It is RFC1583 Compatible
SPF schedule delay 5000 ms
Maximum Number of Equal Cost Paths 4
Number of External LSAs (Type 5) is 6, Checksum is 0x11029BEB
Number of Opaque External LSAs (Type11) is 0, Checksum is 0x0
Number of originated LSAs is 126
Number of received LSAs is 1006
  Area BACKBONE(0)
    Administrative state is UP
    Number of interfaces in this area is 2
    Area has message digest authentication
    SPF algorithm executed 4 times
    Area ranges are
      192.168.0.0/16 Advertise
      192.100.0.0/16 Not Advertise
    Number of ASBR is 0
    Number of ABR is 2
    Number of LSA in this area is 10. Checksum Sum 0x29BEB
    Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
    Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
```

```
     Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
     Number of Summary ASBR LSA(Type 4) 2. Checksum Sum 0x2929BEB
     Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
     Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
 Area 24
     Administrative state is UP
     Number of interfaces in this area is 2
     Area has no authentication
     SPF algorithm executed 10 times
     Area ranges are
     Number of ASBR is 1
     Number of ABR is 3
     Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
     Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
     Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
     Number of Summary ASBR LSA(Type 4) 2. Checksum Sum 0x2929BEB
     Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
     Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
Area 10.0.0.0
     It is a NSSA area
     Administrative state is UP
     Number of interfaces in this area is 4
     Area default metric is 100
      Perform type-7/type-5 LSA translation, suppress forwarding address
     Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
     Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
     Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
     Number of Summary ASBR LSA(Type 4) 2. Checksum Sum 0x2929BEB
     Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
     Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
Area 192.168.1.1
     It is a stub area, no summary
     Administrative state is UP
     Number of interfaces in this area is 4
     Area default metric is 100
     Number of Router LSA(Type 1) 2. Checksum Sum 0x2929BEB
     Number of Network LSA(Type 2) 3. Checksum Sum 0x2929000
     Number of Summary IP Network LSA(Type 3) 3. Checksum Sum 0xBEB
     Number of Opaque Link-Local LSAs (Type 9) is 0, Checksum is 0x0
     Number of Opaque Area-Local LSAs (Type 10) is 0, Checksum is 0x0
```

52.22 show ip ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ip ospf database** command in EXEC mode.

Syntax

show ip ospf [*process-id* [*area-id*]] **database**

show ip ospf [*process-id* [*area-id*]] **database** [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**asbr-summary**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**asbr-summary**] *[link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**database-summary**]

show ip ospf [*process-id* [*area-id*]] **database** [**external**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**external**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**external**] [*link-state-id*] [**self-originate]** [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**network**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**network**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**network**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**nssa-external**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**nssa-external**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**nssa-external**] [*link-state-id]* [**self-originate**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**router**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**router**] [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**router**] [**self-originate**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**self-originate**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**summary**] [*link-state-id*]

show ip ospf [*process-id* [*area-id*]] **database** [**summary**] [*link-state-id*] [**adv-router** [*ip-address*]]

show ip ospf [*process-id* [*area-id*]] **database** [**summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

Parameters

- **process-id**—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
- **area-id**—Area number associated with the OSPF address range defined in the network router configuration command used to define the particular area.
- **adv-router** [*ip-address*]—Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate).

- **link-state-id**—Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.

  When the link state advertisement is describing a network, the link-state-id can take one of two forms:

  The network's IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).

  A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)

  When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.

  When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).
- **asbr-summary**—Displays information only about the autonomous system boundary router summary LSAs.
- **database-summary**—Displays how many of each type of LSA for each area there are in the database, and the total.
- **external**—Displays information only about the external LSAs.
- **network**—Displays information only about the network LSAs.
- **nssa-external**—Displays information only about the NSSA external LSAs.
- **router**—Displays information only about the router LSAs.
- **self-originate**—Displays only self-originated LSAs (from the local router).
- **summary**—Displays information only about the summary LSAs.

Command Mode

User EXEC

User Guidelines

The various forms of this command deliver information about different OSPF link state advertisements.

Example

Example 1. The following is sample output from the show ip ospf database command when no arguments or keywords are used:

```
Router# show ip ospf database


OSPF Routing Process 300 with ID 192.168.239.66


          Displaying Router Link States(Area 0.0.0.0)


Link ID           ADV Router       Age     Seq#          Checksum   Link count
------------------ ---------------  -----   ----------------  ---------------  -----------
172.16.21.6       172.16.21.6      1731   0x80002CFB    0x69BC       8
172.16.21.5       172.16.21.5      1112    0x800009D2    0xA2B8        5
172.16.1.2        172.16.1.2       1662    0x80000A98    0x4CB6       9
172.16.1.1        172.16.1.1       1115    0x800009B6    0x5F2C       1
```

```
172.16.1.5       172.16.1.5         1691      0x80002BC     0x2A1A        5
172.16.65.6      172.16.65.6        1395      0x80001947    0xEEE1        4
172.16.241.5     172.16.241.5       1161      0x8000007C    0x7C70        1
172.16.27.6      172.16.27.6        1723      0x80000548    0x8641        4
172.16.70.6       172.16.70.6       1485      0x80000B97    0xEB84        6

                Displaying Net Link States(Area 0.0.0.0)

Link ID          ADV Router       Age      Seq#          Checksum
------------------  ---------------         -----      ----------------   --------------
172.16.1.3       192.168.239.66     1245    0x800000EC      0x82E

                Displaying Summary Net Link States(Area 0.0.0.0)

Link ID          ADV Router       Age      Seq#          Checksum
------------------  ---------------         -----      ----------------   --------------
172.16.240.0   172.16.241.5      1152   0x80000077      0x7A05
172.16.241.0   172.16.241.5      1152   0x80000070      0xAEB7
172.16.244.0   172.16.241.5       1152  0x80000071      0x95CB
```

Example 2. The following is sample output from the show ip ospf database command with the **asbr-summary** keyword:

```
Router# show ip ospf database asbr-summary

OSPF Routing Process 300 with ID 192.168.239.66

                Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router), Type 4
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 0x80000072
LS Checksum: 0x3548
LS Length: 28
Network Mask: 0.0.0.0
TOS: 0  Metric: 1
```

Example 3. The following is sample output from the show ip ospf database command with the **external** keyword:

```
Router# show ip ospf database external

OSPF Routing Process 300 with ID 192.168.239.66
```

```
                Displaying AS External Link States

LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link, Type 5
Link State ID: 10.105.0.0 (External Network)
Advertising Router: 172.16.70.6
LS Seq Number: 0x80000AFD
LS Checksum: 0xC3A
LS Length: 36
Network Mask: 255.255.0.0
TOS: 0
  Metric Type: 2 (Larger than any link state path)
  Metric: 1
  Forward Address: 0.0.0.0
  External Route Tag: 0
```

Example 4. The following is sample output from the show ip ospf database command with the **network** keyword:

```
Router# show ip ospf database network

OSPF Routing Process 300 with ID 192.168.239.66

             Displaying Network Link States(Area 0.0.0.0)

LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links, Type 2
Link State ID: 172.16.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 0x800000E7
LS Checksum: 0x1229
LS Length: 52
Network Mask: 255.255.255.0
  Attached Router: 192.168.239.66
  Attached Router: 172.16.241.5
  Attached Router: 172.16.1.1
  Attached Router: 172.16.54.5
  Attached Router: 172.16.1.5
```

Example 5. The following is sample output from the show ip ospf database command with the **router** keyword:

```
Router# show ip ospf database router
```

```
OSPF Routing Process 300 with ID 192.168.239.66

Displaying Router Link States(Area 0.0.0.0)

LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links, Type 1
Link State ID: 172.16.21.6
Advertising Router: 172.16.21.6
LS Seq Number: 0x80002CF6
LS Checksum: 0x73B7
LS Length: 120
AS Boundary Router
Number of Links: 8
  Link connected to: another Router (point-to-point)
    Link ID) Neighboring Router ID: 172.16.21.5
    (Link Data) Router Interface address: 172.16.21.6
    Number of TOS metrics: 0
    TOS 0  Metrics: 2
  Link connected to: another Router (transit network
    Link ID) Neighboring Router ID: 182.16.21.5
    (Link Data) Designated Router: 182.18.21.6
    Number of TOS metrics: 0
    TOS 0  Metrics: 2
```

Example 6. The following is sample output from show ip ospf database command with the **summary** keyword:

```
Router# show ip ospf database summary

OSPF Routing Process 300 with ID 192.168.239.66

                Displaying Summary Net Link States(Area 0.0.0.0)

LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network), Type 3
Link State ID: 172.16.240.0 (summary Network Number)
Advertising Router: 172.16.241.5
LS Seq Number: 0x80000072
LS Checksum: 0x84FF
LS Length: 28
Network Mask: 255.255.255.0
```

```
TOS: 0  Metric: 1
```

Example 7. The following is sample output from show ip ospf database command with the **database-summary** keyword:

```
Router# show ip ospf database database-summary


OSPF Routing Process 1 with ID 10.0.1.1


Area 0 database summary
  LSA Type             Count
  Router                  3
  Network                 0
  Summary Net             0
  Summary ASBR            0
  Type-7 Ext              0
  Opaque Link             0
  Opaque Area             0
  Subtotal                3

Process 1 database summary


  LSA Type           Count
  Router                2
  Network               0
  Summary Net           2
  Summary ASBR          0
  Type-7 Ext            0
  Opaque Link           0
  Opaque Area           0
  Opaque AS              0
  Total                  4
```

Example 8. The following is sample output from the show ip ospf database command with the **nssa-external** keyword:

```
Router# show ip ospf database nssa-external


OSPF Routing Process 300 with ID 192.168.239.66


                    Displaying NSSA External Link States


LS age: 280
Options: (No TOS-capability)
LS Type: NSSA External Link, Type 7
Link State ID: 10.105.0.0 (External Network)
```

```
Advertising Router: 172.16.70.6
LS Seq Number: 0x80000AFD
LS Checksum: 0xC3A
LS Length: 36
Network Mask: 255.255.0.0
TOS: 0
  Metric Type: 2 (Larger than any link state path)
  Metric: 1
  Forward Address: 0.0.0.0
  External Route Tag: 0
```

52.23 show ip ospf interface

To display OSPF interface information related to Open Shortest Path First (OSPF), use the **show ip ospf interface** command in user EXEC or privileged EXEC mode.

Syntax

show ip ospf [*process-id*] **interface** [*ip-address*] [**brief**]

Parameters

- **process-id**—Process ID number. If this argument is included, only information for the specified routing process is included. Range is from 1 to 65535.
- **ip-address**—Interface IP address.

brief—Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Mode

EXEC

Privileged EXEC

Example

Example 1. The following is sample output from the **show ip ospf** interface command when Ethernet interface 0/0 is specified:

```
Router# show ip ospf interface

OSPF Routing Process 1 with ID 192.168.0.0

Internet Address 192.168.254.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF Adminastrative state is up
  Cost: 10
  IP Interface has message digest authentication, key chain name is chain99
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
  It is a Designated Router
  Designated Router (ID) 192.168.99.1, Interface address 192.168.254.202
  Backup Designated router (ID) 192.168.254.10, Interface address 192.168.254.10
  Number of LSAs 120, Checksum 0x11029BEB
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.254.10  (Backup Designated Router)
Internet Address 192.168.25.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF Adminastrative state is is up
  It is  a passive interface
  Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
  Designated Router (ID) 192.168.9.10, Interface address 192.168.25.20
  Backup Designated router (ID) 192.168.25.10, Interface address 192.168.25.10
  Transmit Delay is 1 sec
  Number of LSAs 120, Checksum 0x11029BEB
  Neighbor Count is 3, Adjacent neighbor count is 0
Internet Address 192.168.250.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF on interface is down
  It is  a passive interface
  Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
Internet Address 192.168.250.202/24, Area 0
  Interface VLAN 10, BROADCAST is up, IP Interface is down, OSPF Adminastrative state is up
  Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
Internet Address 192.168.50.202/24, Area 0
  Interface VLAN 10, BROADCAST is down, IP Interface is down, OSPF Adminastrative state is up
  Cost: 10
  IP Interface has no authentication
  Transmit Delay is 1 sec
  Priority 1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
```

Example 2. The following sample output from the **show ip ospf interface brief** command shows a summary of information:

```
Router# show ip ospf interface brief
```

```
IP Interface         Process ID Area ID            Cost   Auth Type OSPF Oper St  Passive
-------------------- ------------- --------------------- -------- ------------  ------------------ -----------
172.116.211.116                1 172.116.211.116      10 digest            up             Yes
1.1.2.1                        1              1.1.2.0     35                   down
1.1.3.1                        1                   20     55                    up
```

52.24 show ip ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in privileged EXEC mode.

Syntax

show ip ospf [*process-id*] **neighbor** [**interface** *ip-address*] [*neighbor-id*] [**detail**]

Parameters

- **process-id**—Process ID number. If this argument is included, only information for the specified routing process is included. Range is from 1 to 65535.
- **interface** *ip-address*—Interface IP address.
- **neighbor-id**—Neighbor hostname or IP address in A.B.C.D format.
- **detail**—Displays all neighbors given in detail (lists all neighbors).

Command Mode

Privileged EXEC

Example

Example 1. The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor:

```
Router# show ip ospf neighbor

Neighbor Addr         Neighbor ID      PID    IP Interface       Pri  State        Dead Time
----------------------- --------------------  ----- ---------------------- ---  -------- ------ ---------------
192.199.1199.137 100.199.199.137     1 192.199.199.100 100 Exch/OTH    00:00:31
2.1.1.1                1.1.1.1               2 2.2.2.12              100 TwoW/OTH 00:01:31
3.1.1.1                30.1.1.1              3 2.2.2.12              100 ExSt/OTH    00:01:31
4.1.1.12               40.1.1.1              2 4.2.2.12              100 Exch/OTH 00:01:31
5.1.1.1                50.1.1.1              2 5.2.2.12              100 Load/OTH 00:01:31
6.1.1.1                6.1.1.1               2 6.2.2.12              100 Load/BDR 00:01:31
7.1.1.1                7.1.1.1               2 7.2.2.12              100 Load/DR   00:01:31
```

Example 2. The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
Router# show ip ospf neighbor 10.199.199.137
Neighbor 10.199.199.137, interface address 192.168.80.37
```

```
  Process ID 1, Area 0.0.0.0, Interface 10.199.80.1
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 172.16.48.189
  Process ID 1, Area 0.0.0.0, Interface 172.16.50.19
  Neighbor priority is 5, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:03
```

Example 3. If you specify the interface along with the neighbor ID, the system displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
Router# show ip ospf neighbor interface 192.168.80.100 10.199.199.137
Neighbor 10.199.199.137, interface address 192.168.80.37
  Process ID 1, Area 0.0.0.0, Interface 192.168.80.100
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:37
  Link State retransmission due in 0:00:04
```

Example 4. You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
interface, as in the following sample display:
Router# show ip ospf neighbor interface 172.16.50.1

Neighbor Addr          Neighbor ID      PID   IP Interface      Pri  State       Dead Time
----------------------- ---------------------  ----- ----------------------- ---  -------- ------ ---------------
172.16.50.2            100.199.199.137    1 172.16.50.1         100 Exch/OTH    00:00:31
172.16.50.3            1.1.1.1            1 172.16.50.1          10 TwoW/OTH 00:01:31
172.16.50.4            30.1.1.1           1 172.16.50.1         120 ExSt/OTH    00:01:31
```

Example 5.The following is sample output from the show ip ospf neighbor detail command :

```
Router# show ip ospf neighbor 192.168.5.2 detail
Neighbor 192.168.5.2, interface address 10.225.200.28
  Process ID 1, Area 0.0.0.0, Interface 10.199.80.1
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.225.200.28 BDR is 10.225.200.30
  Options is 0x42
  LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
```

```
Dead timer due in 00:00:36
Number requested LSAs 0
Retransmission queue length 0
```

52.25 show ip ospf router-id

To display OSPF process router-id, use the **show ip ospf router-id** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 ospf [*process-id*] **router-id**

Parameters

process-id—Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.

Default Configuration

Command Mode

Privileged EXEC

EXEC

User Guidelines

The *process-id* argument can be entered as a decimal number or as an IPv6 address format.

Example

The following is sample output from the **show ip ospf router-id** command:

```
show ip ospf router-id

Process-ID      Current Router-ID       Next Router-ID after Restart
                Value             Type     Value             Type
--------------  -------------------  ---------  -------------------  ---------
            1   1.1.1.192          default  1.1.1.1            default
            2   1.1.1.192          default  100.100.100.100  manual
            3   2.2.2.2            manual   2.2.2.2            default
            4   10.10.10.10        manual   1.1.1.1            default
            5   10.10.10.10        manual    2.2.2.2           manual
```

52.26 show ip ospf snmp

To display OSPF snmp configuration, use the **show ip ospf snmp** command in user EXEC or privileged EXEC mode.

Syntax

show ip ospf snmp

Command Mode

Privileged EXEC

EXEC

User Guidelines

Use the **show ipv6 ospf snmp** command to display the OSPF snmp configuration.

Example

The following is sample output from the **show ip ospf snmp** command:

```
show ip ospf snmp

The standard OSPF MIB is mapped to OSPF process 2
SNMP notifications for OSPF are enabled
SNMP notifications Rate Limit: 10 seconds and 7 notifications during the window time
Authentication Failure Notifications are enabled
Bad Packet Notifications are disabled
Configuration Error Notifications are enabled
Virtual Link Authentication-failure Notifications are disabled
Virtual Link Bad Packet Notifications are enabled
Virtual Link Configuration Error Notifications are enabled
SNMP LSA Notifications are disabled
SNMP Packet Retransmission Notifications are disabled
SNMP Virtual Packet Retransmission Notifications are disabled
SNMP IF State Change Notifications are enabled
SNMP Neighbor State Change Notifications are enabled
SNMP Virtual IF State Change Notifications are enabled
SNMP Virtual Neighbor State Change Notifications are enabled
```

52.27 show ip ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ip ospf virtual-links** command in EXEC mode.

Syntax

show ip ospf virtual-links [*process-id*]

Parameters

process-id—Process ID. If this argument is included, only information for the specified routing process is included.

Command Mode

EXEC

User Guidelines

The information displayed by the show ip ospf virtual-links command is useful in debugging OSPF routing operations.

Example

The following is sample output from the show ip ospf virtual-links command:

```
Router# show ip ospf virtual-links


OSPF Routing Process 4 with ID 10.10.24.4


Virtual Link to router 192.168.101.2,  Transit area 0.0.0.1
  Virtual Link State is UP Virtual Link  Cost is 100
  Virtual Link has message digest authentication, key chain name is chain1
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
  Transmit Delay is 1 sec
Virtual Link to router 192.16.10.2, Transit area 10.0.0.1
  Virtual Link State DOWN
  Virtual Link has no authentication
  Hello Interval  is 10  sec, Dead Interval is 40 sec, Retransmit Interval is 5 sec
  Transmit Delay is 1 sec
```

52.28 shutdown (OSPF)

To initiate a graceful shutdown of the Open Shortest Path First (OSPF) protocol under the current instance, use the **shutdown** command in router configuration mode. To restart the OSPF protocol, use the **no** form of this command.

Syntax

shutdown

no shutdown

Parameters

N/A

Default Configuration

OSPF stays active under the current instance.

Command Mode

Router configuration (config-router)

User Guidelines

Use the **shutdown** command in router configuration mode to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path.

The **no shutdown** command changes the OSPF process router-id if it was reconfigured by the user else if the current used router-id has the default value the command runs the router-id re-election algorithm.

Example

The following example shows how to enable a graceful shutdown of the OSPF protocol:

```
router ospf 1
  shutdown
exit
```

52.29 snmp-process ospf

To specify an OSPF process accessed via the standard OSPF MIB, use the **snmp-process ospf** command in global configuration mode. To return to the default, use the **no** form of this command.

Syntax

snmp-process ospf *process-id*

no snmp-process [*process-id*]

Parameters

process-id—OSPF process ID.

Default Configuration

The minimal existed OSPF process.

Command Mode

Global configuration mode

User Guidelines

The standard MIB do not include the OSPF process-ID and by default is mapped to the minimal OSPF process. Use the **snmp-process** command to change the mapping.

Example

The following example maps the standard MIBs to OSPF process 100:

```
snmp-process ospf 100
```

52.30 snmp-server enable traps ospf

To enable all Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF), use the **snmp-server enable traps ospf** command in global configuration mode. To disable all SNMP notifications for OSPF, use the **no** form of this command.

Syntax

snmp-server enable traps ospf

no snmp-server enable traps ospf

Parameters

N/A

Default Configuration

SNMP notifications for OSPF are disabled.

Command Mode

Global configuration

User Guidelines

If you wish to enable or disable specific OSPF SNMP notifications, enter one or more of the following commands of the following commands:

[**no**] **snmp-server enable traps ospf errors**

[**no**] **snmp-server enable traps ospf lsa**

[**no**] **snmp-server enable traps ospf retransmit**

[**no**] **snmp-server enable traps ospf state-change**

Example

The following exampleglobally enables SNMP notifications for OSPF:

```
Router(config)# snmp-server enable traps ospf
```

52.31 snmp-server enable traps ospf errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) errors, use the s**nmp-server enable traps ospf errors** command in global configuration mode. To disable SNMP notifications for OSPF errors, use the **no** form of this command.

Syntax

snmp-server enable traps ospf errors [**authentication-failure**][**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

no snmp-server enable traps ospf errors [**authentication-failure**][**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-bad-packet**] [**virt-config-error**]

Parameters

- **authentication-failure**—Enables only the ospfIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a nonvirtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.
- **bad-packet**—Enables only the ospfIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a nonvirtual interface.
- **config-error**—Enables only the ospfIfConfigError trap. Sends SNMP notifications when a packet has been received in a nonvirtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.
- v**irt-authentication-failure**—Enables only the ospfVirtIfFailure trap. Allows SNMP notifications to be sent when a packet has been received on a virtual interface from a neighbor router whose authentication key or authentication type conflicts with the authentication key or authentication type of this router.

- **virt-bad-packet**—Enables only the ospfVirtIfRxBadPacket trap. Allows SNMP notifications to be sent when an OSPF packet that has not been parsed has been received on a virtual interface.
- **virt-config-error**—Enables only the ospfVirtIfConfigError trap. Sends SNMP notifications when a packet has been received in a virtual interface from a neighbor router whose configuration parameters conflict with the configuration parameters of this router.

Default Configuration

SNMP notifications for OSPF errors are disabled.

Command Mode

Global configuration

User Guidelines

When you enter the **snmp-server enable traps ospf errors** command without any optional keywords, all OSPF error traps will be enabled. To enable only one or more OSPF error traps, enter one or more of the optional keywords.

Example

The following example enables the router to send all OSPF error notifications:

```
Router(config)# snmp-server enable traps ospf errors
```

52.32 snmp-server enable traps ospf lsa

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) link-state advertisements (LSAs), use the **snmp-server enable traps ospf lsa** command in global configuration mode. To disable SNMP notifications for OSPF LSAs, use the **no** form of this command.

Syntax

snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]

no snmp-server enable traps ospf lsa [**lsa-maxage**] [**lsa-originate**]

Parameters

- **lsa-maxage**—Enables the ospfMaxAgeLsa trap
- **lsa-originate**—Enables the ospfOriginateLsa trap

Default Configuration

SNMP notifications for OSPF LSAs are disabled.

Command Mode

Global configuration

User Guidelines

The **snmp-server enable traps ospf lsa** command enables the traps for standard LSAs that are defined by the OSPF-MIB. To enable the ospfMaxAgeLsa trap, enter the **snmp-server enable traps ospf lsa** command with the **lsa-maxage** keyword. To enable the ospfOriginateLsa trap, enter the

snmp-server enable traps ospf lsa command with the **lsa-originate** keyword. When the ospfOriginateLsa trap is enabled, it will not be invoked for simple LSA refreshes that take place every 30 minutes or when an LSA has reached its maximum age and is being flushed. When you enter the **snmp-server enable traps ospf lsa** command without either keyword, both traps will be enabled.

To enable the traps that are defined by the CISCO-OSPF-TRAP-MIB for opaque LSAs, enter the **snmp-server enable traps ospf cisco-specific lsa** command in global configuration mode.

Example

The following example enables the router to send SNMP notifications when new LSAs are originated by the router as a result of a topology change:

```
Router(config)# snmp-server enable traps ospf lsa lsa-originate
```

52.33 snmp-server enable traps ospf rate-limit

To limit the number of Open Shortest Path First (OSPF) traps that are sent during a specified number of seconds, use the **snmp-server enable traps ospf rate-limit** command in global configuration mode. To disable the limit placed on the number of OSPF traps sent during a specified number of seconds, use the **no** form of this command.

Syntax

snmp-server enable traps ospf rate-limit *seconds trap-number*

no snmp-server enable traps ospf rate-limit *seconds trap-number*

Parameters

- **seconds**—Sets the rate limit window size, in seconds. A number from 2 to 60. The default value is 10.
- **trap-number**—Sets the maximum number of traps sent during the window time. A number from 0 to 300. The default number is 7.

Default Configuration

No limit is placed on the number of OSPF traps sent.

Command Mode

Global configuration

User Guidelines

There is a possibility that a router sends trap bursts, which can drain network resources in a small interval of time. It is recommended that you enter the snmp-server enable traps ospf rate-limit command to configure a sliding window mechanism that will limit the number of traps that are sent within a specified number of seconds

Example

he following example sets the trap rate limit window so that during a 40-second window of time, no more that 50 traps are sent:

```
Router(config)# snmp-server enable traps ospf rate-limit 40 50
```

52.34 snmp-server enable traps ospf retransmit

To enable Simple Network Management Protocol (SNMP) notifications when packets are re-sent in an Open Shortest Path First (OSPF) network, use the **snmp-server enable traps ospf retransmit** command in global configuration mode. To disable SNMP notifications, use the **no** form of this command.

Syntax

snmp-server enable traps ospf retransmit [**packets**] [**virt-packets**]

no snmp-server enable traps ospf retransmit [**packets**] [**virt-packets**]

Parameters

- **packets**—Enables only the ospfTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a nonvirtual interface.
- **virt-packets**—Enables only the ospfVirtTxRetransmit trap. Allows SNMP notifications to be sent when an OSPF packet has been re-sent on a virtual interface.

Default Configuration

SNMP notifications are disabled.

Command Mode

Global configuration

User Guidelines

To enable the ospfTXRetransmit trap so that SNMP notifications are sent only when packets from nonvirtual interfaces are re-sent, enter the **snmp-server enable traps ospf retransmit** command with the **packets** keyword. To enable the ospfTxRetransmit trap so that SNMP notifications are sent only when packets from virtual interfaces are re-sent, enter the **snmp-server enable traps ospf retransmit** command with the **virt-packets** keyword. When you enter the **snmp-server enable traps ospf retransmit** command without either keyword, both traps will be enabled.

Example

The following example enables the router to send SNMP notifications when packets are re-sent by virtual interfaces:

```
Router(config)# snmp-server enable traps ospf retransmit virt-packets
```

52.35 snmp-server enable traps ospf state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf state-change** command in global configuration mode. To disable SNMP notifications for OSPF transition state changes, use the **no** form of this command.

Syntax

snmp-server enable traps ospf state-change [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

no snmp-server enable traps ospf state-change [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

Parameters

- **if-state-change**—Enables only the ospfIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF interface.
- **neighbor-state-change**—Enables only the ospfNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a nonvirtual OSPF neighbor.
- **virtif-state-change**—Enables only the ospfVirtIfStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF interface.
- **virtneighbor-state-change**—Enables only the ospfVirtNbrStateChange trap. Sends SNMP notifications when there has been a change in the state of a virtual OSPF neighbor.

Default Configuration

SNMP notifications for OSPF transition state changes are disabled.

Command Mode

Global configuration

User Guidelines

To enable all traps for transition state changes, enter the **snmp-server enable traps ospf state-chang**e command without of the optional keywords.

Example

The following example enables the router to send SNMP notifications for transition state changes for virtual interfaces and virtual neighbors:

```
Router(config)# snmp-server enable traps ospf state-change virtif-state-change
virtneighbor-state-change
```

53 Router Resources Commands

53.1 system router resources

Use the **system router resources** command in Global Configuration mode to configure the system router resources. To return to the default, use the **no** form of this command.

Syntax

system router resources [**ip-entries** *max-number*] [**ipv6-entries** *max-number*] [**ipm-entries** *max-number*] [**ipmv6-entries** *max-number*]

no system router resources

Parameters

- **ip-entries**—The maximum number of IPv4 **entries**.
- **ipv6-entries**—The maximum number of IPv6 **entries**.
- **ipm-entries**—The maximum number of IPv4 **entries** ((*,G) and (S,G)).
- **ipm-entries**—The maximum number of IPv6 **entries** ((*,G) and (S,G)).

Default Configuration

Product specific

Command Mode

Global configuration

User Guidelines

Use the **system router resources** command to enter new settings for routing entries. After entering the command, the current routing entries configuration will be displayed, and the user will be required to confirm saving the new setting to the startup-configuration and to reboot the system.

Data Validation:

If the new settings exceed the maximum number of routing entries, the command is rejected and a message is displayed to the user.

If the new settings are lower than the currently in-use routing entries, a confirmation message is displayed to the user (before the save confirmation message).

Use the **no system router resources** command to the default settings.

The following table displays the conversion between logical entities to HW entries:

Table 5: IPv4

Logical Entity	IPv4
IP Neighbor	1 entry
IP Address	2 entries

Table 5: IPv4

Logical Entity	IPv4
IP Remote Route	1 entry
	2 entries

Table 6: IPv6

Logical Entity	IPv4	IPv6 (PCL TCAM)	IPv6 (Router TCAM)
IP Neighbor	1 entry	1 entry	4 Entries
IP Address	2 entries	2 entries	8 entries
IP Remote Route	1 entry	1 entry	4 Entries
On-Link-Prefix		1 Entry	4 Entries
IPM Group (*,G) or (S,G)	2 entries	2 entries	8 entries

Examples

Example 1

The following example defines the supported number of IPv4 and IPv6 routing entries. In the example, the configured router entries are less than the router entries which are currently in use. Using this configurations means that the system will not have enough resources for the running again in the existing network:

```
switchxxxxxx#system router resources ip-routes 128 ipv6-routes 32
The maximal number of IPv4 Routing entries and IPv6 Routing Entries is
3072. The number is Non-IP Entries is 3096.
                             In-Use   Reserved (Current)  Reserved (New)
                             ------   ------------------  --------------
IPv4 Entries                   232          1024               128
     Number of Routes           20
     Number of Neighbors        12
     Number of Interfaces      100
IPv6 Entries                  1024          1024                32
     Number of Routes           20
     Number of Neighbors        12
     Number of Interfaces      100
     Number of On-Link Prefixes  1
IPv4 Multicast                   0           0                   0
Michael If the IPv6 Multicast Router is supported
IPv6 Multicast                   0           0                   0
Non-IP Entries:
- Unit 1                     93%         400
- Unit 2                         94%          400
- Unit 5                         90%          400
The new configuration of route entries is less than the route entries
which are currently in use by the system, do you want to continue (note
that setting the new configuration of route entries requires saving the
running-configuration file to startup-configuration file and rebooting the
system)? (Y/N) [N] Y
```

Example 2

The following example defines the supported number of IPv4 routing entries.

```
switchxxxxxx#system router resources ip-routes 256



The maximal number of IPv4 and IPv6 Routing Entries is 3072. The number is
Non-IP Entries is 3096.

                            In-Use  Reserved (Current)  Reserved (New)
                            ------  ------------------  --------------
IPv4 Entries                   232        1024                256
     Number of Routes           20
     Number of Neighbors        12
     Number of Interfaces      100


Non-IP Entries:
- Unit 1               93%          400
- Unit 2               94%          400
- Unit 5               90%          400
Setting the new configuration of route entries requires saving the
running-configuration file to startup-configuration file and rebooting the
system, do you want to continue? (Y/N) [N] Y
```

53.2 show system router resources

Use the **show system router resources** command in EXEC mode to display the router resources.

Syntax

show system router resources

Parameters

This command has no arguments or keywords.

Command Mode

EXEC mode

Example

Example 1. In the following example, the configured router entries are displayed:

```
switchxxxxxx#show system router resources
The maximal number of IPv4 and IPv6 Routing Entries is 3072. The number is
Non-IP Entries is 3096.
                        In-Use            Reserved
                        ------            --------
IPv4 Entries                232                1024
     Number of Routes       20
     Number of Neighbors    12
     Number of Interfaces  100
IPv4 Multicast               0                  0
IPv6 Multicast               0                  0
Non-IP Entries:
- Unit 1          93%         400
- Unit 2          94%         400
- Unit 5          90%         400
```

54 MLD Commands

54.1 clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the **clear ipv6 mld counters** command in privileged EXEC mode.

Syntax

clear ipv6 mld counters [*interface-id*]

Parameters

interface-id—Interface Identifier

Command Mode

Privileged EXEC

User Guidelines

Use the **clear ipv6 mld counters** command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional *interface-id* argument, the **clear ipv6 mld counters** command clears the counters on all interfaces.

Example

The following example clears the counters for VLAN 100:

```
clear ipv6 mld counters vlan 100
```

54.2 ipv6 mld access-group

To perform IPv6 multicast receiver access control, use the **ipv6 mld access-group** command in interface configuration mode. To stop using multicast receiver access control, use the **no** form of this command.

Syntax

ipv6 mld access-group *access-list*

no ipv6 mld access-group

Parameters

access-list—A pair IP6 named access list that defines the multicast groups and sources to allow or deny.

Default Configuration

All groups and sources are allowed.

Command Mode

Interface configuration

User Guidelines

The **ipv6 mld access-group** command is used for receiver access control and to check the groups and sources in Multicast Listener Discovery (MLD) reports against the access list. The **ipv6 mld access-group** command also limits the state created by MLD reports. The **ipv6 mld access-group** command allows users to limit the list of groups a receiver can join.

If an IGMP report with (S1, S2...Sn, G) is received, first the group (0, G) is checked against the access list statements. If the group is denied, the entire MLD report is denied. If the group is permitted, each individual (S, G) pair is checked against the access list. Denied sources are taken out of the MLD report, thereby denying any sources that match the access list from sending to the group.

Example

Example 1. The following example creates an access list called acc-grp-1 and denies all the state for group ff04::10 on VLAN 100:

```
ipv6 access-list pair acc-grp-1 permit ipv6 any ff04::10
interface vlan 100
  ipv6 mld access-group acc-grp-1
exit
```

Example 2. The The following example permits only EXCLUDE(G,{}) reports. This example converts EXCLUDE(G,{S1, S2..Sn}) into EXCLUDE(G,{}) on VLAN 100:

```
ipv6 access-list pair acc-grp-1 permit any ff04::10 ::
ipv6 access-list pair acc-grp-1 deny any ff04::10 any
ipv6 access-list pair acc-grp-1 permit any any
!
interface vlan 100
  ipv6 mld access-group acc-grp-1
exit
```

Example 3. The following example filters a particular source 100::1 for a group ff04::10 on VLAN 100:

```
ipv6 access-list pair acc-grp-1 deny any ff04::10 100::1
ipv6 access-list pair acc-grp-1 permit any ff04::10
!
interface vlan 100
  ipv6 mld access-group acc-grp-1
exit
```

54.3 ipv6 mld last-member-query-interval

To configure the Multicast Listener Discovery (MLD) last member query interval, use the **ipv6 mld last-member-query-interval** command in interface configuration mode. To restore the default MLD query interval, use the **no** form of this command.

Syntax

ipv6 mld last-member-query-interval *milliseconds*

no ipv6 mld last-member-query-interval

Parameters

milliseconds—Interval, in milliseconds, at which MLD group-specific host query messages are sent on the interface. (Range: 100–25500)

Default Configuration

The default MLD last member query interval is 1000 milliseconds.

Command Mode

Interface configuration

User Guidelines

Use the **ipv6 mld last-member-query-interval** command to configure the MLD last member query interval on an interface.

Example

The following example shows how to increase the the MLD last member query interval to 1500 milliseconds:

```
interface vlan 100
  ipv6 mld last-member-query-interval 1500
exit
```

54.4 ipv6 mld query-interval

To configure the frequency at which the switch sends Multicast Listener Discovery (MLD) host-query messages, use the **ipv6 mld query-interval** command in interface configuration mode. To return to the default frequency, use the **no** form of this command.

Syntax

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

Parameters

seconds—Frequency, in seconds, at which the switch sends MLD query messages from the interface. The range is from 1 to 31744.

Default Configuration

The default MLD query interval is 125 seconds.

Command Mode

Interface configuration

User Guidelines

Use the **ipv6 mld query-interval** command to configure the frequency at which the MLD querier sends MLD host-query messages from an interface. The MLD querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

The query interval must be bigger than the maximum query response time.

Example

The following example shows how to increase the frequency at which the MLD querier sends MLD host-query messages to 180 seconds:

```
interface vlan 100
  ipv6 mld query-interval 180
exit
```

54.5 ipv6 mld query-max-response-time

To configure the maximum response time advertised in Multicast Listener Discovery (MLD) queries, use the **ipv6 mld query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

Parameters

seconds—Maximum response time, in seconds, advertised in MLD queries. (Range: 0–3174)

Default Configuration

10 seconds.

Command Mode

Interface configuration

User Guidelines

This command controls the period during which the responder can respond to an MLD query message before the router deletes the group.

This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

The maximum query response time must be less than the query interval.

Note. If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

The following example configures a maximum response time of 8 seconds:

```
interface vlan 100
  ipv6 mld query-max-response-time 8
exit
```

54.6 ipv6 mld robustness

To configure the Multicast Listener Discovery (MLD) robustness variable, use the **ipv6 mld robustness** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ipv6 mld robustness *count*

no ipv6 mld robustness

Parameters

count—The number of expected packet loss on a link. Parameter range. (Range: 1–7)

Default Configuration

The default value is 2.

Command Mode

Interface configuration

User Guidelines

Use the **ipv6 mld robustness** command to change the MLD robustness variable.

Example

The following example changes a value of the MLD robustness variable to 3:

```
interface vlan 1
  ipv6 mld robustness 3
exit
```

54.7 ipv6 mld version

To configure which version of Multicast Listener Discovery Protocol (MLD) the router uses, use the **ipv6 mld version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ipv6 mld version {**1** | **2**}

no ipv6 mld version

Parameters

1—MLD Version 1.

2—MLD Version 2.

Default Configuration

Version 2

Command Mode

Interface configuration

User Guidelines

Use the commnad to change the default version of MLD.

Example

The following example configures the router to use MLD Version 1:

```
interface vlan 100
  ipv6 mld version 1
exit
```

54.8 show ipv6 mld counters

To display the Multicast Listener Discovery (MLD) traffic counters, use the **show ipv6 mld counters** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 mld counters [*interface-id*]

Parameters

interface-id—Interface Identifier

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ipv6 mld counters** command to check if the expected number of MLD protocol messages have been received and sent.

If you omit the optional *interface-id* argument, the **show ipv6 mld counters** command displays counters of all interfaces.

Example

The following example displays the MLD protocol messages received and sent:

```
show ipv6 mld counters vlan 100

VLAN 100
   Elapsed time since counters cleared:00:00:21
   Failed received Joins: 0
   Total MLDv1 received messages: 10
   Total MLDv2 received messages: 0
   Total invalid received messages: 0
   General Sent Queries: 0
   Specific Sent Queries: 0
```

54.9 show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the **show ipv6 mld groups** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 mld groups [**link-local**] [*group-name* | *group-address*] [*interface-id*] [**detail**]

Parameters

link-local—Displays the link-local groups.

group-name | group-address—IPv6 address or name of the multicast group.

interface-id—Interface identifier.

detail—Displays detailed information about individual sources.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

If you omit all optional arguments, the **show ipv6 mld groups** command displays by group address and interface-id all directly connected multicast groups, including link-local groups (where the link-local keyword is not available) used.

Example

Example 1. The following is sample output from the **show ipv6 mld groups** command. It shows all of the groups joined by VLAN 100:

```
show ipv6 mld groups vlan 100

MLD Connected Group Membership
Expires: never - switch itself has joined the group

Group Address                       Interface     Expires
FF02::2                             VLAN 100      never
FF02::1:FF00:1                      VLAN          00:10:27
FF02::1:FFAF:2C39                   VLAN 100      00:09:11
FF06:7777::1                        VLAN 100      00:00:26
```

Example 2. The following is sample output from the **show ipv6 mld groups** command using the **detail** keyword:

```
show ipv6 mld groups detail

Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state

Interface: VLAN 100
 Group: FF33::1:1:1
  Router mode: INCLUDE
  Last reporter: 2009:5::12:1
  Group Timer Expires: 00:20:11
  Group source list:
  Source Address                        Expires
  2004:4::6                             00:00:11
  2004:4::16                            00:08:11
 Group: FF33::1:1:2
  Router mode: EXCLUDE
  Last reporter: 2008:5::2A:10
  Group Timer Expires: 00:20:11
  Exclude Mode Expiry (Filter) Timer: 00:10:11
  Group source list:
  Source Address                        Expires
  2004:5::1                             00:04:08
  2004:3::1                             00:04:08
  2004:7::10                            00:00:00
  2004:50::1                            00:00:00
```

54.10 show ipv6 mld groups summary

To display the number of (*, G) and (S, G) membership reports present in the Multicast Listener Discovery (MLD) cache, use the **show ipv6 mld groups summary** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 mld groups summary

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ipv6 mld groups summary** command displays the number of directly connected multicast groups (including link-local groups).

Example

The following is sample output from the **show ipv6 mld groups summary** command:

```
show ipv6 mld groups summary


MLD Route Summary
   No. of (*,G) routes = 5
   No. of (S,G) routes = 0
```

Field Descriptions:

No. of (*,G) routes = 5—Displays the number of groups present in the MLD cache.

No. of (S,G) routes = 0—Displays the number of include and exclude mode sources present in the MLD cache.

54.11 show ipv6 mld interface

To display multicast-related information about an interface, use the **show ipv6 mld interface** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 mld interface [*interface-id*]

Parameters

interface-id—Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

If you omit the optional *interface-id* argument, the **show ipv6 mld interface** command displays information about all interfaces.

Example

The following is sample output from the **show ipv6 mld interface** command for Ethernet interface 2/1/1:

```
show ipv6 mld interface vlan 100


VLAN 100 is up
    Administrative MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
```

```
Operational MLD Querier IPv6 address is FE80::260:3EFF:FE86:5649
Current MLD version is 3
Administrative MLD robustness variable is 2 seconds
Operational MLD robustness variable is 2 seconds
Administrative MLD query interval is 125 seconds
Operational MLD query interval is 125 seconds
Administrative MLD max query response time is 10 seconds
Operational MLD max query response time is 10 seconds
Administrative Last member query response interval is 1000 milliseconds
Operational Last member query response interval is 1000 milliseconds
```

55 IGMP Commands

55.1 clear ip igmp counters

To clear theInternet Group Management Protocol (IGMP) interface counters, use the **clear ip igmp counters** command in privileged EXEC mode.

Syntax

clear ip igmp counters [*interface-id*]

Parameters

interface-id—Interface Identifier

Command Mode

Privileged EXEC

User Guidelines

Use the **clear ip igmp counters** command to clear the IGMP counters, which keep track of the number of joins and leaves received. If you omit the optional *interface-id* argument, the **clear ip igmp counters** command clears the counters on all interfaces.

Example

The following example clears the counters for VLAN 100:

```
clear ip igmp counters vlan 100
```

55.2 ip igmp access-group

To perform IP multicast receiver access control, use the **ip igmp access-group** command in interface configuration mode. To stop using multicast receiver access control, use the **no** form of this command.

Syntax

ip igmp access-group *access-list*

no ip igmp access-group

Parameters

access-list—A pair IP named access list that defines the multicast groups and sources to allow or deny.

Default Configuration

All groups and sources are allowed.

Command Mode

Interface configuration

User Guidelines

The **ip igmp access-group** command is used for receiver access control and to check the groups and sources in Internet Group Management Protocol (IGMP) reports against the access list. The **ip igmp access-group** command also limits the state created by IGMP reports. The **ip igmp access-group** command allows users to limit the list of groups a receiver can join.

If an IGMP report with (S1, S2...Sn, G) is received, first the group (0, G) is checked against the access list statements. If the group is denied, the entire IGMP report is denied. If the group is permitted, each individual (S, G) pair is checked against the access list. Denied sources are taken out of the IGMP report, thereby denying any sources that match the access list from sending to the group.

Example

Example 1. The following example shows how to configure a pair access list to filter the groups that are available on an interface for receivers to join. In this example, Ethernet interface 1/3 is configured to restrict receivers from joining groups in the range 226.1.0.0 through 226.1.255.255. Receivers are permitted to join all other groups on VLAN 100:

```
ip access-list pair 1 deny any 226.1.0.0/16
ip access-list pair 1 permit any any
!
interface vlan 100
  ip igmp access-group 1
exit
```

Example 2. The following example shows how to deny all states for a group G. In this example, VLAN 100 is configured to filter all sources for SSM group 232.2.2.2 in IGMPv3 reports, which effectively denies this group:

```
ip access-list pair test1 deny any 232.2.2.2
ip access-list pair test1 permit any any
!
interface vlan 100
  ip igmp access-group test1
exit
```

Example 3. The following example shows how to deny all states for a source S. In this example, VLAN 100 is configured to filter all groups for source 10.2.1.32 in IGMPv3 reports, which effectively denies this source:

```
ip access-list pair test2 deny 10.2.1.32
ip access-list pair test1 permit any any
!
interface vlan 100
  ip igmp access-group test2
exit
```

Example 4. The following example shows how to permit all states for a group G. In this example, VLAN 100 is configured to accept all sources for SSM group 232.1.1.10 in IGMPv3 reports, which effectively accepts this group altogether:

```
ip access-list pair test3 permit any 232.1.1.10

interface vlan 100
  ip igmp access-group test3
exit
```

Example 5. The following example shows how to permit all states for a source S. In this example, VLAN 100 is configured to accept all groups for source 10.6.23.32 in IGMPv3 reports, which effectively accepts this source altogether:

```
ip access-list pair test4 permit 10.6.23.32 any
!
interface vlan 100
  ip igmp access-group test4
exit
```

Example 6. The following example shows how to filter a particular source S for a group G. In this example, VLAN 100 is configured to filter source 232.2.2.2 for SSM group 232.2.30.30 in IGMPv3 reports:

```
ip access-list pair test5 deny 10.4.4.4 232.2.30.30
ip access-list pair test1 permit any any
!
interface vlan 100
  ip igmp access-group test5
exit
```

55.3 ip igmp last-member-query-interval

To configure the Internet Group Management Protocol (IGMP) last member query interval, use the **ip igmp last-member-query-interval** command in interface configuration mode. To restore the default IGMP query interval, use the **no** form of this command.

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

The default IGMP last member query interval is 1000 milliseconds.

Command Mode

Interface configuration

User Guidelines

Use the **ip igmp last-member-query-interval** command to configure the IGMP last member query interval on an interface.

Example

The following example shows how to increase the the IGMP last member query interval to 1500 milliseconds:

```
interface vlan 100
  ip igmp last-member-query-interval 1500
exit
```

55.4 ip igmp query-interval

To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the **ip igmp query-interval** command in interface configuration mode. To restore the default IGMP query interval, use the **no** form of this command.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval

Parameters

seconds—Frequency, in seconds, at which the switch sends IGMP query messages from the interface. The range is from 1 to 31744.

Default Configuration

The default IGMP query interval is 125 seconds.

Command Mode

Interface configuration

User Guidelines

Use the **ip igmp query-interval** command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

The query interval must be bigger than the maximum query response time.

Example

The following example shows how to increase the frequency at which the IGMP querier sends IGMP host-query messages to 180 seconds:

```
interface vlan 100
  ip igmp query-interval 180
exit
```

55.5 ip igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **ip igmp query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ip igmp query-max-response-time *seconds*

no ip query-max-response-time

Parameters

seconds—Maximum response time, in seconds, advertised in IGMP queries. (Range: 0–3174)

Default Configuration

10 seconds.

Command Mode

Interface configuration

User Guidelines

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

This command controls how much time the hosts have to answer an IGMP query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster.

The maximum query response time must be less than the query interval.

Note. If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

The following example configures a maximum response time of 8 seconds:

```
interface vlan 100
  ip igmp query-max-response-time 8
exit
```

55.6 ip igmp robustness

To configure the Internet Group Management Protocol (IGMP) robustness variable, use the **ip igmp robustness** command in interface configuration mode. To restore the default value, use the **no** form of this command.

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

The default value is 2.

Command Mode

Interface configuration

User Guidelines

Use the **ip igmp robustness** command to change the IGMP robustness variable.

Example

The following example changes a value of the IGMP robustness variable to 3:

```
interface vlan 1
  ip igmp robustness 3
exit
```

55.7 ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Parameters

1—IGMP Version 1.

2—IGMP Version 2.

3—IGMP Version 3.

Default Configuration

Version 3

Command Mode

Interface configuration

User Guidelines

Use the commnad to change the default version of IGMP>

Example

The following example configures the router to use IGMP Version 2:

```
interface vlan 100
  ip igmp version 2
exit
```

55.8 show ip igmp counters

To display the Internet Group Management Protocol (IGMP) traffic counters, use the **show ip igmp counters** command in user EXEC or privileged EXEC mode.

Syntax

show ip igmp counters [*interface-id*]

Parameters

interface-id—Interface Identifier

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip igmp counters** command to check if the expected number of IGMP protocol messages have been received and sent.

If you omit the optional *interface-id* argument, the **show ip igmp counters** command displays counters of all interfaces.

Example

The following example displays the IGMP protocol messages received and sent:

```
show ip igmp counters vlan 100

VLAN 100
   Elapsed time since counters cleared:00:00:21
   Failed received Joins: 0
   Total IGMPv1 received messages: 0
   Total IGMPv2 received messages: 10
   Total IGMPv3 received messages: 0
   Total invalid received messages: 0
   General Sent Queries: 0
   Specific Sent Queries: 0
```

55.9 show ip igmp groups

To display the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP) , use the **show ip igmp groups** command in user EXEC or privileged EXEC mode.

Syntax

show ip igmp groups [*group-name* | *group-address*] [*interface-id*] [**detail**]

Parameters

group-name | group-address—IP address or name of the multicast group.

interface-id—Interface identifier.

detail—Displays detailed information about individual sources.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

If you omit all optional arguments, the **show ip igmp groups** command displays by group address and interface-id all directly connected multicast groups.

Example

Example 1. The following is sample output from the **show ip igmp groups** command. It shows all of the groups joined by VLAN 100:

```
show ip igmp groups vlan 100

IGMP Connected Group Membership
Expires: never - switch itself has joined the group

Group Address                       Interface     Expires
224.1.1.1                           VLAN  100     00:01:30
224.10.12.79                        VLAN  100     never
225.1.1.1                           VLAN 100      00:00:27
```

Example 2. The following is sample output from the **show ip igmp groups** command using the **detail** keyword:

```
show ip igmp groups detail
```

```
Expires: zero value - INCLUDE state; non-zero value - EXCLUDE state

Interface: VLAN 100
 Group: 225.1.1.1
  Router mode: INCLUDE
  Last reporter: 10.0.119.133
  Group Timer Expires: 00:20:11
  Group source list:
  Source Address                    Expires
  20.1.1.1                          00:04:08
  120.1.1.1                         00:02:01
 Group: 226.1.1.2
  Router mode: EXCLUDE
  Last reporter: 100.1.12.130
  Group Timer Expiry: 00:22:12
  Exclude Mode Expiry (Filter) Timer: 00:10:11
  Group source list:
  Source Address                    Expires
  2.2.2.1                          00:04:08
  192.168.1.1                      00:04:08
  12.1.1.10                        00:00:00
  40.3.4.2                         00:00:00
```

55.10 show ip igmp groups summary

To display the number of (*, G) and (S, G) membership reports present in the Internet Group Management Protocol (IGMP) cache, use the **show ip igmp groups summary** command in user EXEC or privileged EXEC mode.

Syntax

show ip igmp groups summary

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ip igmp groups summary** command displays the number of directly connected multicast groups.

Example

The following is sample output from the **show ip igmp groups summary** command:

```
show ip igmp groups summary


IGMP Route Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 0
```

Field Descriptions:

No. of (*,G) routes = 5—Displays the number of groups present in the IGMP cache.

No. of (S,G) routes = 0—Displays the number of include and exclude mode sources present in the IGMP cache.

55.11 show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** command in user EXEC or privileged EXEC mode.

Syntax

show ip igmp interface [*interface-id*]

Parameters

interface-id—Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

If you omit the optional *interface-id* argument, the **show ip igmp interface** command displays information about all interfaces.

Example

The following is sample output from the **show ip igmp interface** command for Ethernet interface 2/1/1:

```
show ip igmp interface vlan 100


VLAN 100 is up
   Administrative IGMP Querier IP address is 1.1.1.1
   Operational IGMP Querier IP address is 1.1.1.1
   Current IGMP version is 3
   Administrative IGMP robustness variable is 2 seconds
```

```
Operational IGMP robustness variable is 2 seconds
Administrative IGMP query interval is 125 seconds
Operational IGMP query interval is 125 seconds
Administrative IGMP max query response time is 10 seconds
Operational IGMP max query response time is 10 seconds
Administrative Last member query response interval is 1000 milliseconds
Operational Last member query response interval is 1000 milliseconds
```

56 IPv4 IPM Router Commands

56.1 ip multicast-routing

To enable the multicast routing on all IP-enabled interfaces of the router and to enable multicast forwarding, use the **ip multicast-routing** command in global configuration mode. To stop multicast routing and forwarding, use the **no** form of this command.

Syntax

ip multicast-routing [**pim** | **igmp-proxy**]

no ip multicast-routing

Parameters

pim—Enable multicast routing using Protocol Independent Multicast (PIM).

igmp-proxy—Enable multicast routing using IGMP Proxy.

Default Configuration

Multicast routing is not enabled.

Command Mode

Global configuration

User Guidelines

Use the **ip multicast-routing** command with parameter to specify the needed IP Multicast Routing Protocol. The **ip multicast-routing** command without parameter enables PIM.

To be IPV6 multicast packets forwarded on an interface the IP multicast forwarding must be enabled globally and an IPM Routing protocol must be enabled on the interface.

Example

The following example enables IP multicast routing using IGMP Proxy:

```
ip multicast-routing igmp-proxy
```

56.2 ip multicast ttl-threshold

To configure the time-to-live (TTL) threshold of packets being forwarded out an interface, use the **ip multicast ttl-threshold** command in interface configuration mode. To return to the default TTL threshold, use the **no** form of this command.

Syntax

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold

Parameters

ttl-value—Time-to-live value, in hops. It can be a value from 0 to 256.

Default Configuration

The default TTL value is 0.

Command Mode

Interface configuration

User Guidelines

Multicast packets with a TTL value less than the threshold will not be forwarded out the interface.

The default value of 0 means all multicast packets are forwarded out the interface.

A value of 256 means that no multicast packets are forwarded out the interface.

You should configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

Example

The following example sets the TTL threshold on a border router to 200:

```
interface vlan 100
  ip multicast ttl-threshold 200
exit
```

56.3 show ip mroute

To display the contents of the multicast routing (mroute) table, use the **show ip mroute** command in user EXEC or privileged EXEC mode.

Syntax

show ip mroute [*group-address* [*source-address*]] [**summary**]

Parameters

group-address—IP address or Domain Name System (DNS) name of a multicast group.

source-address—IP address or DNS name of a multicast source.

summary—Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip mroute** command to display information about mroute entries in the mroute table. The switch populates the multicast routing table by creating (S, G) entries from (*, G) entries. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the switch uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Example

Description of Significant fields

Flags:—Provides information about the entry.

- S—Sparse. Entry is operating in sparse mode.
- X—IGMP Proxy.
- s—SSM Group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
- C—Connected. A member of the multicast group is present on the directly connected interface.
- L—Local. The router itself is a member of the multicast group.
- R—RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source.
- F—Register flag. Indicates that the software is registering for a multicast source.
- T—SPT-bit set. Indicates that packets have been received on the shortest path source tree.
- J—Join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree.

  For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

  Note. The router measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

  If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest path source tree when traffic from a new source is received.
- I—Received Source Specific Host Report. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by Internet Group Management Protocol Version 3 (IGMPv3), URD, or IGMP v3lite. This flag is set only on the designated router (DR).

Timers:Uptime/Expires—“Uptime” indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. “Expires” indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.

(*, 224.0.255.1) and (192.168.37.100/32, 224.0.255.1)—Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources.

Entries in the first format are referred to as (*, G) or “star comma G” entries. Entries in the second format are referred to as (S, G) or “S comma G” entries. (*, G) entries are used to build (S, G) entries.

flags:—Information about the entry.

Incoming interface: —Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.

RPF neighbor or RPF nbr—IP address of the upstream router to the source. Tunneling indicates that this router is sending data to the RP encapsulated in register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used. If an asterisk (*) appears after the IP address in this field, the RPF neighbor has been learned through an assert.

Outgoing interface list:—Interfaces through which packets will be forwarded.

Example 1. The following is sample output from the **show ip mroute** command:

```
show ip mroute

IP Multicast Routing Table

Flags: S - Sparse, X - IGMP Proxy,s - SSM Group,
       C - Connected, L - Local, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: vlan2, RPF neighbor 10.3.35.1
  Outgoing interface list:
    vlan100, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: vlan2, RPF neighbor 10.3.35.1
  Outgoing interface list:
    vlan5, 5:29:15/0:02:57
```

Example 2. The following is sample output from the **show ip mroute** command with the IP multicast group address 232.6.6.6 specified:

```
show ip mroute 232.6.6.6

IP Multicast Routing Table

Flags: S - Sparse, X - IGMP Proxy,s - SSM Group,
       C - Connected, L - Local, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires
Timers: Uptime/Expires

(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 224.0.0.0
  Outgoing interface list:Null
(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags:CTI
  Incoming interface:vlan33, RPF nbr 224.0.0.0
  Outgoing interface list:
    vlan30, 00:00:36/00:02:35
```

Example 3. The following is sample output from the **show ip mroute** command with the summary keyword:

```
show ip mroute summary

IP Multicast Routing Table

Flags: S - Sparse, X - IGMP Proxy,s - SSM Group,
       C - Connected, L - Local, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

(*, 224.255.255.255), 2d16h/00:02:30, RP 172.16.10.13, OIF count:1, flags: SJ
(*, 224.2.127.253), 00:58:18/00:02:00, RP 172.16.10.13, OIF count:2, flags: SJC
(*, 224.1.127.255), 00:58:21/00:02:03, RP 172.16.10.13, OIF count:2, flags: SJ
(*, 224.2.127.254), 2d16h/00:00:00, RP 172.16.10.13, OIF count:2, flags: SJCL
  (172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, OIF count:2, flags: CLJT
  (172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, OIF count:2, flags: CLJT
  (172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, OIF count:2, flags: CLJT
  (172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, OIF count:2, flags: CLJT
  (172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, OIF count:2, flags: CLJT
  (172.16.60.189/32, 224.2.127.254), 00:03:47/00:00:46, OIF count:2, flags: CLJT
```

56.4 show ip multicast

To display general information about IP multicast, use the **show ip multicast** command in user EXEC or privileged EXEC mode.

Syntax

show ip multicast [**interface** *interface-id*]

Parameters

interface—Displays IP multicast-related information about an interface configured for IP multicast.

interface-id—Interface identifier for which to display IP multicast information.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip multicas**t command without the **interface** keyword to display general information about the state of IP multicast on the router.

Use the **show ip multicast** command with the **interface** keyword to display the IP multicast information about the interface.

Example

Example 1. The following is sample output from the **show ip multicast** command without the **interface** keyword when no IP Multicast Routing protocol is enabled:

```
show ip multicast

IP Unicast Forwarding: enabled
IP Multicast Protocol: No
```

Example 2. The following is sample output from the **show ip multicast** command without the **interface** keyword when IGMP Proxy is enabled:

```
show ip multicast

IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
```

Example 3. The following is sample output from the **show ip multicast** command about the given interface, IGMP Proxy is enabled on the interface and the interface an IGMP Proxy Upstream interface:

```
show ip multicast interface vlan 200

IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
 TTL-threshold: 0
 IGMP Protocol: IGMPv3
 PIM: disabled
 IGMP Proxy: Upstream
```

Example 4. The following is sample output from the **show ip multicast** command about the given interface, IGMP Proxy is enabled on the interface and the interface is an IGMP Proxy Downlink interface:

```
show ip multicast interface vlan 100

IP Unicast Forwarding: enabled
IP Multicast Protocol: PIM
vlan 200
 TTL-threshold: 0
 IGMP Protocol: IGMPv3
 PIM: enabled
 IGMP Proxy: DownStream (Upstream: vlan 200)
```

57 IPv6 IPM Router Commands

57.1 ipv6 multicast-routing

To enable the multicast routing on all IPv6-enabled interfaces of the router and to enable multicast forwarding, use the **ipv6 multicast-routing** command in global configuration mode. To stop multicast routing and forwarding, use the **no** form of this command.

Syntax

ipv6 multicast-routing [**pim** | **mld-proxy**]

no ipv6 multicast-routing

Parameters

pim—Enable multicast routing using Protocol Independent Multicast (PIM).

mld-proxy—Enable multicast routing using MLD Proxy.

Default Configuration

Multicast routing is not enabled.

Command Mode

Global configuration

User Guidelines

Use the **ipv6 multicast-routing** command with parameter to specify the needed IP Multicast Routing Protocol. The **ipv6 multicast-routing** command without parameter enables PIM.

To be IPV6 multicast packets forwarded on an interface the IPv6 multicast forwarding must be enabled globally and an IPMv6 Routing protocol must be enabled on the interface.

Example

The following example enables IPv6 multicast routing using MLD Proxy:

```
ipv6 multicast-routing mld-proxy
```

57.2 ipv6 multicast hop-threshold

To configure the Hop Limit threshold of packets being forwarded out an interface, use the **ipv6 multicast hop-threshold** command in interface configuration mode. To return to the default Hop Limit threshold, use the **no** form of this command.

Syntax

ip multicast hop-threshold *hop-value*

no ip multicast hop-threshold

Parameters

hop-value—Hop Limit value. It can be a value from 0 to 256.

Default Configuration

The default Hop Limit value is 0.

Command Mode

Interface configuration

User Guidelines

Multicast packets with a hop value less than the threshold will not be forwarded out the interface.

The default value of 0 means all multicast packets are forwarded out the interface.

A value of 256 means that no multicast packets are forwarded out the interface.

You should configure the hop threshold only on border routers. Conversely, routers on which you configure a hop threshold value automatically become border routers.

Example

The following example sets the Hop Limit threshold on a border router to 200:

```
interface vlan 100
  ipv6 multicast hop-threshold 200
exit
```

57.3 show ipv6 mroute

To display the contents of the multicast routing (mroute) table, use the **show ipv6 mroute** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 mroute [*group-address* [*source-address*]] [**summary**]

Parameters

group-address—IPv6 address or Domain Name System (DNS) name of a multicast group.

source-address—IPv6 address or DNS name of a multicast source.

summary—Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip mroute** command to display information about mroute entries in the mroute table. The switch populates the multicast routing table by creating (S, G) entries from (*, G) entries. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the switch uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Example

Description of Significant fields

Flags:—Provides information about the entry.

- S—Sparse. Entry is operating in sparse mode.
- X—MLD Proxy.
- s—SSM Group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
- C—Connected. A member of the multicast group is present on the directly connected interface.
- L—Local. The router itself is a member of the multicast group.
- R—RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source.
- F—Register flag. Indicates that the software is registering for a multicast source.
- T—SPT-bit set. Indicates that packets have been received on the shortest path source tree.
- J—Join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree.

  For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

  Note. The router measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

  If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest path source tree when traffic from a new source is received.
- I—Received Source Specific Host Report. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by Internet Group Management Protocol Version 3 (IGMPv3), URD, or IGMP v3lite. This flag is set only on the designated router (DR).

Timers:Uptime/Expires—“Uptime” indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. “Expires” indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.

(*, FF07::1) and (FF07::1/128, FF07::1)—Entry in the IPv6 multicast routing table. The entry consists of the IP address of the source router followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources.

Entries in the first format are referred to as (*, G) or “star comma G” entries. Entries in the second format are referred to as (S, G) or “S comma G” entries. (*, G) entries are used to build (S, G) entries.

flags:—Information about the entry.

Incoming interface: —Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.

RPF neighbor or RPF nbr—IP address of the upstream router to the source. Tunneling indicates that this router is sending data to the RP encapsulated in register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used. If an asterisk (*) appears after the IP address in this field, the RPF neighbor has been learned through an assert.

Outgoing interface list:—Interfaces through which packets will be forwarded.

Example 1. The following is sample output from the show ipv6 mroute command:

```
show ip mroute

IP Multicast Routing Table

Flags: S - Sparse, X - MLD Proxy,s - SSM Group,
       C - Connected, L - Local, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface: vlan5, RPF nbr:6:6:6::6
  Outgoing interface list:
    vlan40, Forward, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface: vlan10, RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    vlan40, Forward, 00:02:06/00:03:27
```

Example 2. The following is sample output from the show ip mroute command with the IP multicast group address FF07::1 specified:

```
show ip mroute

IP Multicast Routing Table

Flags: S - Sparse, X - MLD Proxy,s - SSM Group,
       C - Connected, L - Local, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface: vlan5, RPF nbr:6:6:6::6
  Outgoing interface list:
    vlan40, Forward, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface: vlan10, RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    vlan40, Forward, 00:02:06/00:03:27
```

Example 3. The following is sample output from the **show ipv6 mroute** command with the summary keyword:

```
show ip mroute summary

IP Multicast Routing Table

Flags: S - Sparse, X - MLD Proxy,s - SSM Group,
       C - Connected, L - Local, R - RP-bit set,
       F - Register flag, T - SPT-bit set, J - Join SPT,
       I - Received Source Specific Host Report
Timers: Uptime/Expires

(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, OIF count:1, flags:S
(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT
```

57.4 show ipv6 multicast

To display general information about IPv6 multicast, use the **show ipv6 multicast** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 multicast [**interface** [*interface-id*]]

Parameters

interface—Displays IPv6 multicast-related information about interfaces configured for IP multicast.

interface-id—Interface identifier for which to display IPv6 multicast information.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ipv6 multicas**t command without the **interface** keyword to display general information about the state of IP multicast on the router.

Use the **show ipv6 multicast** command with the **interface** keyword to display the IP multicast information about the interface.

Example

Example 1. The following is sample output from the **show ipv6 multicast** command without the **interface** keyword when no IPv6 Multicast Routing protocol is enabled:

```
show ipv6 multicast

IPv6 Unicast Forwarding: enabled
IP Multicast Protocol: No
```

Example 2. The following is sample output from the **show ipv6 multicast** command without the **interface** keyword when MLD Proxy is enabled:

```
show ipv6 multicast

IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
```

Example 3. The following is sample output from the **show ipv6 multicast** command about the given interface, MLD Proxy is enabled on the interface and the interface is an MLD Proxy Upstream interface:

```
show ipv6 multicast interface vlan 200

IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
vlan 200
 IPv6 Status: enabled
 hop-threshold: 0
 MLD Protocol: MLDv2
 PIM: disabled
 MLD Proxy: Upstream
```

Example 4. The following is sample output from the **show ipv6 multicast** command about the given interface, MLD Proxy is enabled on the interface and the interface is an MLD Proxy Downlink interface:

```
show ipv6 multicast interface vlan 100

IPv6 Unicast Forwarding: enabled
```

```
IPv6 Multicast Protocol: PIM
vlan 200
 IPv6 Status: disabled
 hop-threshold: 0
 MLD Protocol: IGMPv3
 PIM: enabled
 MLD Proxy: DownStream (Upstream: vlan 200)
```

Example 5. The following is sample output from the **show ipv6 multicast** command about the given interface, MLD Proxy is disabled on the interface:

```
show ipv6 multicast interface vlan 100


IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: No
vlan 200
 IPv6 Status: enabled
 hop-threshold: 100
 MLD Protocol: IGMPv3
 PIM: enabled
 MLD Proxy: disabled
```

58 IPv4 PIM Commands

58.1 clear ip pim counters

To reset the Protocol Independent Multicast (PIM) traffic counters, use the **clear ip pim counters** command in privileged EXEC mode.

Syntax

clear ip pim counters

Parameters

N/A

Command Mode

Privileged EXEC

User Guidelines

Using the **clear ip pim counters** command will reset all PIM traffic counters.

Example

The following example resets the PIM traffic counters:

```
clear ip pim counters
```

58.2 ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

Syntax

ip pim

no ip pim

Parameters

N/A

Default Configuration

PIM is automatically enabled on every interface.

Command Mode

Interface configuration

User Guidelines

After a user has enabled the **ip multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ip pim** command to disable PIM on a specified interface.

Example

The following example turns off PIM on VLAN 100:

```
interface vlan 100
  no ip pim
exit
```

58.3 ip pim accept-register

To configure a candidate rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

Syntax

ip pim accept-register list *access-list*

no ip pim accept-register list

Parameters

acces-list—Defines the IP pair access list name.

Default Configuration

The command is disabled.

Command Mode

Global configuration

User Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

Example

The following example shows how to deny register packets for source addresses 10.1.1.0/24 and 172.100.1.1 sending to the 232.0.0.0/8 group range. All other PIM register messages not matching the pair access list are permitted. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first hop routers:

```
ip pim accept-register list no-range
ip access-list pair no-range deny 10.1.1.0/24 232.0.0.0/8
ip access-list pair no-range deny 172.100.1.1 232.0.0.0/8
ip access-list pair no-range permit any any
```

58.4 ip pim bsr-border

To configure a border for all bootstrap message (BSMs) on a specified interface, use the **ip pim bsr-border** command in interface configuration mode. To remove the border, use the **no** form of this command.

Syntax

ip pim bsr-border

no ip pim bsr-border

Parameters

N/A

Default Configuration

No border is configured.

Command Mode

Interface configuration

User Guidelines

The **ip pim bsr-border** command is used to configure a border. The command filters incoming or outgoing BSMs, preventing the BSMs from being forwarded or accepted on the interface on which the **ip pim bsr-border** command is configured.

When this command is configured on an interface, no Protocol Independent Multicast (PIM) Version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Note. This command does not set up multicast boundaries. It sets up only a PIM domain BSR message border.

Example

The following example configures a BSR border on VLAN 100:

```
interface vlan 100
  ip pim bsr-border
exit
```

58.5 ip pim bsr-candidate

To configure a router to be a candidate bootstrap router (BSR), use the **ip pim bsr-candidate** command in global configuration mode. To remove this router as a candidate BSR, use the **no** form of this command.

Syntax

ip pim bsr-candidate *ip-address* [*hash-mask-length*] [**priority** *priority-value*]

no ip pim bsr-candidate

Parameters

- **ip-address**—The IP address of the router to be configured as a candidate BSR.
- **hash-mask-length**—Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups. The default value is 30.
- **priority**—Priority of the candidate BSR.
- **priority-value**—Integer from 0 through 192. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

Default Configuration

Router is not enabled as a BSR.

Command Mode

Global configuration

User Guidelines

The **ip pim bsr-candidate** command is used to configure a router as a candidate BSR. When a router is configured, it will participate in BSR election. If elected BSR, this router will periodically originate BSR messages advertising the group-to-RP mappings it has learned through candidate-RP-advertisement messages.

Example

The following example configures the router with the IPv6 address 112.8.3.3 as the candidate BSR, with a hash mask length of 24 and a priority of 10:

```
ip pim bsr-candidate 112.8.3.3 24 priority 10
```

58.6 ip pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ip pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ip pim dr-priority *value*

no ip pim dr-priority

Parameters

value—An integer value to represent DR priority. Value range is from 0 to 4294967294.

Default Configuration

Default value is 1.

Command Mode

Interface configuration

User Guidelines

The **ip pim dr-priority** command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IP address on the interface becomes the DR.

If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IP address becomes the DR.

Example

The following example configures the router to use DR priority 3:

```
interface vlan 100
  ip pim dr-priority 3
exit
```

58.7 ip pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ip pim hello-interval** command in interface configuration mode. To return to the default interval, use the no form of this command.

Syntax

ip pim hello-interval *seconds*

no ip pim hello-interval

Parameters

seconds—Interval, in seconds, at which PIM hello messages are sent. The range is from 1 to 18000.

Default Configuration

Hello messages are sent at 30-second intervals with small random jitter.

Command Mode

Interface configuration

User Guidelines

Periodic hello messages are sent out at 30-second intervals with a small jitter. The **ip pim hello-interval** command allows users to set a periodic interval.

Example

The following example sets the PIM hello message interval to 45 seconds:

```
interface vlan 100
  ip pim hello-interval 45
```

```
exit
```

58.8 ip pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ip pim join-prune-interval** command in interface configuration mode. To return to the default value, use the **no** form of the command.

Syntax

ip pim join-prune-interval *seconds*

no ip pim join-prune-interval

Parameters

seconds—The join and prune announcement intervals, in number of seconds. The range is from 1 to 18000.

Default Configuration

The default is 60 seconds.

Command Mode

Interface configuration

User Guidelines

The **ip pim join-prune-interval** command allows users to set a periodic interval. The configured PIM join/prune interval also determines the join/prune hold time used by a PIM router as follows:

3.5 * join/prune interval

Example

The following example sets the join and prune announcement intervals to 75 seconds:

```
interface vlan 100
  ip pim join-prune-interval 75
exit
```

58.9 ip pim neighbor-filter

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IP addresses, use the **ip pim neighbor-filter** command in the interface configuration mode. To return to the router default, use the **no** form of this command.

Syntax

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter

Parameters

access-list—Name of an IP standard access list that denies PIM hello packets from a source. The name may contain maximum 32 characters.

Default Configuration

PIM neighbor messages are not filtered.

Command Mode

Interface configuration

User Guidelines

The **ip pim neighbor-filter** command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

Example

The following example causes PIM to ignore all hello messages from IP address 10.1.1.1:

```
interface vlan 100
  ip6 pim neighbor-filter nbr_filter_acl
exit
ip access-list nbr_filter_acl deny 10.1.1.1
ip access-list nbr_filter_acl permit any
```

58.10 ip pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

Syntax

ip pim rp-address *rp-address* [*group*-access-list]

no ip pim rp-address *rp-address*

Parameters

- **rp-address**—The IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.
- **group-access-list**—Name of an IP standard access list that defines for which multicast groups the RP should be used. The name may contain maximum 32 characters.

  If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range, a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges.

  To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address.

Default Configuration

No PIM RPs are preconfigured.

Command Mode

Global configuration

User Guidelines

Groups in sparse mode need to have the IP address of one router to operate as the RP for the group. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

PIM learns RP addresses of multicast groups through the following three mechanisms: static configuration, and bootstrap router (BSR). Use the **ip pim rp-address** command to statically define the RP address for multicast groups.

You can configure PIM to use a single RP for more than one group. The conditions specified by the access list determine for which groups the RP can be used. If no access list is configured, the RP is used for all groups. A PIM router can use multiple RPs, but only one per group.

If multiple **ip pim rp-address** commands are configured, the following rules apply to a multicast group:

- Highest RP IP address selection: If a group is matched by the access list of more than one **ip pim rp-address** command whose prefix masks are all the same lengths, then the mode and RP for the group are determined by the ip pim rp-address command with the highest RP address parameter.
- Static evaluation: The mode and RP selection for a group are static and do not depend on the reachability of the individual RPs. The router will not start using an RP with a lower IP address or a shorter prefix length match if the better RP is not reachable.
- One IP address per command: An IP address can be used as a parameter for only one **ip pim rp-address** command. If an **ip pim rp-address** command is configured with an IP address parameter that was previously used to configure an older **ip pim rp-address** command, then this old command will be replaced with the newly configured command.
- One access list per command: A specific access list can be used as a parameter for only one ip pim rp-address command. If an **ip pim rp-address** command is configured with an access list parameter that was previously used to configure an older ip pim rp-address command, then this old command will be replaced with the newly configured command.

Static definitions for the group mode and RP address of the **ip pim rp-address** command may be used together with dynamically learned group mode and RP address mapping through BSR. The mappings statistically defined by the **ip pim rp-address** command take precedences over mappings learned through BSR.

Example

Example 1. The following example shows how to set the PIM RP address to 192.168.0.0 for all multicast groups and defines all groups to operate in sparse mode:

ip pim rp-address 192.168.0.0:

```
ip pim rp-address 192.168.0.0
```

Example 2. The following example shows how to set the PIM RP address to 172.16.0.0 for the multicast group 225.2.2.2 only:

```
ip access-list acc-grp-1 permit 225.2.2.2
ip pim rp-address 172.16.0.0 acc-grp-1
```

58.11 ip pim rp-candidate

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap router (BSR), use the **ip pim rp-candidate** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the no form of this command.

Syntax

ip pim rp-candidate *rp-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*]

no ip pim rp-candidate *ipv6-address*

Parameters

- **rp-address**—The IP address of the router to be advertised as the candidate RP (C-RP).
- **group-list**—List of group prefixes. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
- **access-list-name**—Name of the IP standard access list containing group prefixes that will be advertised in association with the RP address. If the access list contains any group address ranges that overlap the assigned SSM group address range, a warning message is displayed, and the overlapping address ranges are ignored.
- **priority**—Priority of the candidate BSR.
- **priority-value**—Integer from 0 through 192. The RP with the higher priority is preferred. If the priority values are the same, the router with the higher IPv6 address is the RP. The default value is 192.
- **interval**—Configures the C-RP advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
- **seconds**—Advertisement interval in number of seconds.

Default Configuration

Router is not enabled as a candidate RP.

Command Mode

Global configuration

User Guidelines

Use the **ipv6 pim rp-candidate** command to send PIM RP advertisements to the BSR.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority** *priority-value* keyword and argument are specified, then the router will announce itself to be a candidate RP with the specified priority.

Example

The following example shows how to configure the router to advertise itself as a candidate RP to the BSR in its PIM domain. Standard access list list1 specifies the group prefix associated with the 100.1.1.1 RP address. That RP is responsible for the groups with the prefix 239.0.0.0/8:

```
ip pim rp-candidate 100.1.1.1 group-list list1
ip access-list list permit 239.0.0.0/8
```

58.12 ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

Syntax

ip pim ssm {**default** | **range** *access-list*}

no ip pim ssm

Parameters

- **default**—Defines the SSM range access list to 232/8.
- **range** *access-list*—Specifies the standard IP access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global configuration

User Guidelines

Use the **no ip pim ssm** command to remove all defined ranges.

Example

The following example shows how to configure SSM service for the default IP address range and the IP address ranges defined by access lists **list1** and **list2** :

```
ip access-list list1 permit 224.2.151.0/24
ip access-list list1 deny 224.2.152.141
ip access-list list1 permit 224.2.152.0/24
ip pim ssm range list1
```

58.13 show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

Syntax

show ip pim bsr {**election** | **rp-cache** | **candidate-rp**}

Parameters

- **election**—Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.
- **rp-cache**—Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.

- **candidate-rp**—Displays C-RP state on routers that are configured as C-RPs.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip pim bsr** command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP cache is displayed only on the elected BSR router, and information on the C-RP state machine is displayed only on a router configured as a C-RP.

Example

Example 1. The following example displays BSM election information:

```
show ip pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: 232.1.1.0/24
This system is the Bootstrap Router (BSR)
BSR Address: 110.60.1.4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: 160.1.1.1,vlan0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 110.2.1.4, priority: 0, hash mask length: 126
```

Description of Significant fields

Scope Range List—Scope range list to which this BSR information applies.

This system is the Bootstrap Router (BSR)—Indicates this router is the BSR and provides information on the parameters associated with it.

BS Timer—On the elected BSR, the BS timer shows the time in which the next BSM will be originated. On all other routers in the domain, the BS timer shows the time at which the elected BSR expires.

This system is candidate BSR—Indicates this router is the candidate BSR and provides information on the parameters associated with it.

Example 2. The following example displays information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the `232.1.1.0/24` or the default IP multicast range:

```
show ip pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) 232.1.1.0/24, RP count 2
```

```
  RP 12.1.1.3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20.1.1.1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

Example 3. The following example displays information about the C-RP:

```
show ip pim bsr candidate-rp
PIMv2 C-RP information
  Candidate RP: 10.1.1.3
    Priority 192, Holdtime 150
    Advertisement interval 60 seconds
    Next advertisement in 00:00:33
```

58.14 show ip pim counters

To display the Protocol Independent Multicast (PIM) counters, use the **show ip pim counters** command in user EXEC or privileged EXEC mode.

Syntax

show ip pim counters

Parameters

N/A

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip pim counters** command to check if the expected number of PIM protocol messages have been received and sent.

Example

The following example shows the number of PIM protocol messages received and sent:

```
show ip pim counters
iPIM Traffic Counters
Elapsed time since counters cleared: 00:05:29
                       Received    Sent
Valid PIM Packets            22      22
Hello                        22      22
```

```
Join-Prune                     0       0
Register                       0       0
Register Stop                  0       0
Assert                         0       0
Bootstrap                      0       0
Errors:
Send Errors                                 0
Bad Checksums                               0
Packets Received on PIM-disabled Interface 0
Packets Received with Unknown PIM Version  0
```

58.15 show ip pim group-map

To display an IPv6 Protocol Independent Multicast (PIM) group mapping table, use the **show ip pim group-map** command in user EXEC or privileged EXEC mode

Syntax

show ip pim group-map [*group-address*]

Parameters

group-address—IP address of the multicast group.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip pim group-map** command without the *group-address* argument to display mapping of all groups.

Example

The following example displays information about all groups:

```
show ip pim group-map

Group(s) 226.0.0.0/8
  SM RP 10.10.0.1 (?)
  Info source: Local
Group(s) 227.0.0.0/8
  SM RP 10.10.0.2 (?)
  Info source: Static
Group(s) 228.0.0.0/8
  SM RP 10.10.0.3 (?)
  Info source: From BSR 10.10.0.3 (?), Priority: 192
  Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
```

```
  SM RP 10.10.0.5 (mcast1.aaaa.com)
  Info source: From BSR 10.10.0.5 (mcast1.aaaa.com), Priority: 192
  Uptime:00:00:52, expires:00:00:37
Group(s) 232.0.0.0/8
  SMM
```

58.16 show ip pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in privileged EXEC mode.

Syntax

show ip pim interface [**state-on** | **state-off** | *interface-id*]

Parameters

- **state-on**—Displays interfaces with PIM enabled (adminastrative mode).
- **state-off**—Displays interfaces with PIM disabled(adminastrative mode).
- **interface-id**—Display the interface with the Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ipv6 pim interface** command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

Example

Example 1. The following example displays only PIM state on interfaces:

```
show ip pim interface
IP Forwarding is enabled
IP Multicast Routing is enabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface  Address           Status
vlan 1     1.1.1.1           disabled
vlan 100   102.1.1.1         enabled
vlan 102   160.1.1.1         enabled
vlan 103                     enabled
```

Example 2. The following is sample output from the **show ip pim interface** command using the **state-on** keyword when IP Multicast Routing is disabled:

```
show ip pim interface state-on

IP Forwarding is enabled
IP Multicast Routing is disabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface Status    Nbr     Hello    Join-Prune  DR
                    Count   Intvl    Intvl       Prior
vlan 1    disabled
   Address: 102.1.1.1
   DR:
   Neighbor Filter List: filt
vlan 100  disabled
   Address: 102.1.1.1
   DR:
   Neighbor Filter List: nbr-filter
vlan 102  enabled
   Address: 160.1.1.1
   DR:
   Neighbor Filter List:
vlan 103  enabled
   Address:
   DR:
   Neighbor Filter List: filter1
```

Example 3. The following is sample output from the **show ip pim interface** command using the **state-on** keyword:

```
show ip pim interface state-on

IP Forwarding is enabled
IP Multicast Routing is enabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface Statuse  Nbr     Hello    Join-Prune  DR
                   Count   Intvl    Intvl       Prior
vlan 100  enabled      0      30      60          1
   Address: 102.1.1.1
   DR: this system
   Neighbor Filter List: nbr-filter
vlan 102  enabled      1      30      60          1
   Address: 160.1.1.1
   DR: 160.1.1.10
   Neighbor Filter List:
vlan 103  enabled
   Address:
   DR:
   Neighbor Filter List: filter1
```

Example 4. The following is sample output from the **show ip pim interface** command using the i*nterface-id* argument:

```
show ip pim interface vlan 100
IP Forwarding is enabled
IP Multicast Routing is enabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface Statuse  Nbr     Hello    Join-Prune  DR
                   Count   Intvl    Intvl       Prior
vlan 100  enabled      0      30      60          1
   Address: 102.1.1.1
   DR: this system
   Neighbor Filter List: nbr-filter
```

58.17 show ip pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by the switch, use the **show ip pim neighbor** command in user EXEC or privileged EXEC mode.

Syntax

show ip pim neighbor [**detail**] [*interface-id*]

Parameters

- **detail**—Displays the additional addresses of the neighbors learned, if any, through the Address List (type 24) Hello option.
- **interface-id**—Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ipv6 pim neighbor** command displays which routers on the LAN are configured for PIM.

Example

The following is sample output from the **show ip pim neighbor** command using the detail keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
show ip pim neighbor detail
Neighbor Address(es)   Interface  Uptime   Expires  DR pri
10.1.1.1               vlan 100   01:34:16 00:01:16   1
60.1.1.3
10.1.1.4               vlan 140   01:34:15 00:01:18   1
60.1.1.4
```

58.18 show ip pim rp mapping

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp mapping** command in user EXEC or privileged EXEC mode.

Syntax

show ip pim rp mapping [*rp-address*]

Parameters

rp-address—RP IP address.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ip pim rp mapping** command with the *rp-address* argument to display information about the given RP.

Use the **show ip pim rp mapping** command without the *rp-address* argument to display information about all known RPs.

Example

The following example displays information about all known all RPs:

```
show ip pim rp mapping
This system is an RP
Register Acces List: list1
Group(s) 226.0.0.0/8
  RP 10.10.0.1 (?)
  Info source: Local
  Uptime: 00:02:40
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?)
  Info source: Static
  Uptime: 00:01:42
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?)
  Info source: From BSR 10.10.0.3 (?), Priority: 192
  Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.aaaa.com)
  Info source: From BSR 10.10.0.5 (mcast1.aaaa.com), Priority: 192
  Uptime:00:00:52, expires:00:00:37
```

59 IPv6 PIM Commands

59.1 clear ipv6 pim counters

To reset the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim counters** command in privileged EXEC mode.

Syntax

clear ipv6 pim counters

Parameters

N/A.

Command Mode

Privileged EXEC

User Guidelines

Using the **clear ipv6 pim counters** command will reset all PIM traffic counters.

Example

The following example resets the PIM traffic counters:

```
clear ipv6 pim counters
```

59.2 ipv6 pim

To enable IPv6 Protocol Independent Multicast (PIM) on an interface, use the **ipv6 pim** command in interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

Syntax

ipv6 pim

no ipv6 pim

Parameters

This command has no arguments or keywords.

Default Configuration

PIM is automatically enabled on every IPv6 interface.

Command Mode

Interface configuration

User Guidelines

After a user has enabled the **ipv6 multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface.

Example

The following example turns off PIM on VLAN 100:

```
interface vlan 100
  no ipv6 pim
exit
```

59.3 ipv6 pim accept-register

To configure a candidate rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the **ipv6 pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

Syntax

ipv6 pim accept-register list *access-list*

no ipv6 pim accept-register list

Parameters

acces-list—Defines the IPv6 pair access list name.

Default Configuration

The command is disabled.

Command Mode

Global configuration

User Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

Example

The following example shows how to deny register packets for source addresses 2001:1:1::/48 and 2001:1:10::1 sending to the FF07:1:1:1::/48 group range. All other PIM register messages not matching the pair access list are permitted. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first hop routers:

```
ip6 pim accept-register list no-range
ip6 access-list pair no-range deny 2001:1:1::/48 FF07:1:1:1::/48
ip6 access-list pair no-range deny 2001:1:10::1 FF07:1:1:1::/48
ip6 access-list pair no-range permit any any
```

59.4 ipv6 pim bsr-border

To configure a border for all bootstrap message (BSMs) on a specified interface, use the **ipv6 pim bsr-border** command in interface configuration mode. To remove the border, use the **no** form of this command

Syntax

- ipv6 pim bsr-border
- no ipv6 pim bsr-border

Parameters

N/A.

Default Configuration

No border is configured.

Command Mode

Interface configuration

User Guidelines

The **ipv6 pim bsr-border** command is used to configure a border. The command filters incoming or outgoing BSMs, preventing the BSMs from being forwarded or accepted on the interface on which the **ipv6 pim bsr-border** command is configured.

When this command is configured on an interface, no Protocol Independent Multicast (PIM) Version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Note. This command does not set up multicast boundaries. It sets up only a PIM domain BSR message border.

Example

The following example configures a BSR border on VLAN 100:

```
interface vlan 100
  ipv6 pim bsr-border
exit
```

59.5 ipv6 pim bsr-candidate

To configure a router to be a candidate bootstrap router (BSR), use the **ipv6 pim bsr-candidate** command in global configuration mode. To remove this router as a candidate BSR, use the **no** form of this command.

Syntax

ipv6 pim bsr-candidate *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]

no ipv6 pim bsr-candidate

Parameters

- **ipv6-address**—The IPv6 address of the router to be configured as a candidate BSR. This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.
- **hash-mask-length**—Length of a mask (128 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 126, only the first 126 bits of the group addresses matter. This fact allows you to get one RP for multiple groups. The default value is 126.
- **priority**—Priority of the candidate BSR.
- **priority-value**—Integer from 0 through 192. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR. The default value is 0.

Default Configuration

Router is not enabled as a BSR.

Command Mode

Global configuration

User Guidelines

The **ipv6 pim bsr-candidate** command is used to configure a router as a candidate BSR. When a router is configured, it will participate in BSR election. If elected BSR, this router will periodically originate BSR messages advertising the group-to-RP mappings it has learned through candidate-RP-advertisement messages.

Example

The following example configures the router with the IPv6 address 2001:0DB8:3000:3000::42 as the candidate BSR, with a hash mask length of 124 and a priority of 10:

```
ipv6 pim bsr-candidate 2001:0DB8:3000:3000::42 124 priority 10
```

59.6 ipv6 pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ipv6 pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ipv6 pim dr-priority *value*

no ipv6 pim dr-priority

Parameters

value—An integer value to represent DR priority. Value range is from 0 to 4294967294.

Default Configuration

Default value is 1.

Command Mode

Interface configuration

User Guidelines

The **ipv6 pim dr-priority** command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IPv6 address on the interface becomes the DR.

If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address becomes the DR.

Example

The following example configures the router to use DR priority 3:

```
interface vlan 100
  ipv6 pim dr-priority 3
exit
```

59.7 ipv6 pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ipv6 pim hello-interval** command in interface configuration mode. To return to the default interval, use the no form of this command.

Syntax

ipv6 pim hello-interval *seconds*

no ipv6 pim hello-interval

Parameters

seconds—Interval, in seconds, at which PIM hello messages are sent. The range is from 1 to 18000.

Default Configuration

Hello messages are sent at 30-second intervals with small random jitter.

Command Mode

Interface configuration

User Guidelines

Periodic hello messages are sent out at 30-second intervals with a small jitter. The ipv6 pim hello-interval command allows users to set a periodic interval.

Example

The following example sets the PIM hello message interval to 45 seconds:

```
interface vlan 100
  ipv6 pim hello-interval 45
```

```
exit
```

59.8 ipv6 pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ipv6 pim join-prune-interval** command in interface configuration mode. To return to the default value, use the **no** form of the command.

Syntax

ipv6 pim join-prune-interval *seconds*

no ipv6 pim join-prune-interval

Parameters

seconds—The join and prune announcement intervals, in number of seconds. The range is from 1 to 18000.

Default Configuration

The default is 60 seconds.

Command Mode

Interface configuration

User Guidelines

The **ipv6 pim join-prune-interval** command allows users to set a periodic interval. The configured PIM join/prune interval also determines the join/prune hold time used by a PIM router as follows:

3.5 * join/prune interval

Example

The following example sets the join and prune announcement intervals to 75 seconds:

```
interface vlan 100
  ipv6 pim join-prune-interval 75
exit
```

59.9 ipv6 pim neighbor-filter

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the **ipv6 pim neighbor-filter** command in the interface configuration mode. To return to the router default, use the **no** form of this command.

Syntax

ipv6 pim neighbor-filter *access-list*

no ipv6 pim neighbor-filter

Parameters

access-list—Name of an IPv6 standard access list that denies PIM hello packets from a source. The name may contain maximum characters.

Default Configuration

PIM neighbor messages are not filtered.

Command Mode

Interface configuration

User Guidelines

The **ipv6 pim neighbor-filter** command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

Example

The following example causes PIM to ignore all hello messages from IPv6 address FE80::A8BB:CCFF:FE03:7200:

```
interface vlan 100
  ipv6 pim neighbor-filter nbr_filter_acl
exit
ipv6 access-list deny nbr_filter_acl FE80::A8BB:CCFF:FE03:7200
ipv6 access-list permit nbr_filter_acl any
```

59.10 ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

Syntax

ipv6 pim rp-address *rp-address* [*group-access-list*]

no ipv6 pim rp-address *rp-address*

Parameters

- **rp-address**—The IPv6 address of a router to be a PIM RP. The ipv6-address argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.
- **group-access-list**—Name of an IPv6 standard access list that defines for which multicast groups the RP should be used. The name may contain maximum 32 characters.

  If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range, a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges.

  To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address.

Default Configuration

No PIM RPs are preconfigured.

Embedded RP support is enabled by default when IPv6 PIM is enabled

Command Mode

Global configuration

User Guidelines

Groups in sparse mode need to have the IP address of one router to operate as the RP for the group. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional *group-access-list* argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM (FF3E::/32). If the *group-access-list* argument is specified, the IPv6 address is the RP address for the group range specified in the *group-access-list* argument.

You can configure switch to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

Static definitions for the group mode and RP address of the **ipv6 pim rp-address** command may be used together with dynamically learned group mode and RP address mapping through BSR. The mappings statistically defined by the **ipv6 pim rp-address** command take precedences over mappings learned through BSR.

Static definitions for the group mode and RP address of the **ipv6 pim rp-address** command may be used together with enabling of embedded RP support. The mappings statistically defined by the **ipv6 pim rp-address** command take precedences over embedded RP support.

Example

Example 1. The following example shows how to set the PIM RP address to 2001::10:10 for all multicast groups:

```
ipv6 pim rp-address 2001::10:10
```

Example 2. The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
ipv6 access-list acc-grp-1 permit ff04::/64
ipv6 pim rp-address 2001::10:10 acc-grp-1
```

Example 3. The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
ipv6 access-list embd-ranges permit ff73:240:2:2:2::/96
ipv6 access-list embd-ranges permit ff74:240:2:2:2::/96
ipv6 access-list embd-ranges permit ff75:240:2:2:2::/96
ipv6 access-list embd-ranges permit ff76:240:2:2:2::/96
```

```
ipv6 access-list embd-ranges permit ff77:240:2:2:2::/96
ipv6 access-list embd-ranges permit ff78:240:2:2:2::/96
```

59.11 ipv6 pim rp-candidate

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap router (BSR), use the **ipv6 pim rp-candidate** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the no form of this command.

Syntax

ipv6 pim rp-candidate *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*]

no ipv6 pim rp-candidate *ipv6-address*

Parameters

- **ipv6-address**—The IPv6 address of the router to be advertised as the candidate RP (C-RP). This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.
- **group-list**—List of group prefixes. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
- **access-list-name**—Name of the IPv6 standard access list containing group prefixes that will be advertised in association with the RP address. If the access list contains any group address ranges that overlap the assigned SSM group address range, a warning message is displayed, and the overlapping address ranges are ignored.
- **priority**—Priority of the candidate BSR.
- **priority-value**—Integer from 0 through 192. The RP with the higher priority is preferred. If the priority values are the same, the router with the higher IPv6 address is the RP. The default value is 192.
- **interval**—Configures the C-RP advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
- **seconds**—Advertisement interval in number of seconds.

Default Configuration

Router is not enabled as a candidate RP.

Command Mode

Global configuration

User Guidelines

Use the **ipv6 pim rp-candidate** command to send PIM RP advertisements to the BSR.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority** *priority-value* keyword and argument are specified, then the router will announce itself to be a candidate RP with the specified priority.

Example

Example 1. The following example configures the router with the IPv6 address 2001:0DB8:3000:3000::42 to be advertised as the candidate RP, with a priority of 0:

```
ipv6 pim rp-candidate 2001:0DB8:3000:3000::42 priority 0
```

Example 2. The following example configures the router with the IPv6 address 2001:0DB8:1:1:1 as the candidate RP for the group ranges specified in the access list named list1:

```
ipv6 pim rp-candidate 2001:0DB8:1:1:1 group-list list1
```

59.12 ipv6 pim rp-embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded** command in global configuration mode. To disable embedded RP support, use the no form of this command.

Syntax

ipv6 pim rp-embedded

no ipv6 pim rp-embedded

Parameters

This command has no arguments or keywords.

Default Configuration

Embedded RP support is enabled by default.

Command Mode

Global configuration

User Guidelines

Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support (see RFC 3956 about details).

The **ipv6 pim rp-embedded** command applies only to the embedded RP group addresses defined by RFC3956. When the feature is enabled, the IP Multicast router parses a embedded RP group address and extracts the RP to be used from the group address.

Example

The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp-embedded
```

59.13 ipv6 pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ipv6 pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

Syntax

ipv6 pim ssm {**default** | **range** *access-list*}

no ipv6 pim ssm

Parameters

default—Defines the SSM range access list to FF3E::/32.

range *access-list*—Specifies the standard IPv6 access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global configuration

User Guidelines

To define a few ranges, configure the **ipv6 pim ssm** command a few times.

Use the **no ipv6 pim ssm** command without the keywords to remove all defined ranges.

Example

The following example shows how to configure SSM service for the default IPv6 address range and the IPv6 address ranges defined by access lists **list1** and **list2** :

```
ipv6 access-list list1 permit FF7E:1220:2001:DB8::/64
ipv6 access-list list1 deny FF7E:1220:2001:DB1::1
ipv6 access-list list1 permit FF7E:1220:2001:DB1::/64
ipv6 pim ssm range list1
```

59.14 show ipv6 pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ipv6 pim bsr** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 pim bsr {**election** | **rp-cache** | **candidate-rp**}

Parameters

- **election**—Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.
- **rp-cache**—Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.
- **candidate-rp**—Displays C-RP state on routers that are configured as C-RPs.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ipv6 pim bsr** command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP cache is displayed only on the elected BSR router, and information on the C-RP state machine is displayed only on a router configured as a C-RP.

Example

Example 1. The following example displays BSM election information:

```
show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,VLAN 10
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

Description of Significant fields

Scope Range List—Scope to which this BSR information applies.

This system is the Bootstrap Router (BSR)—Indicates this router is the BSR and provides information on the parameters associated with it.

BS Timer—On the elected BSR, the BS timer shows the time in which the next BSM will be originated. On all other routers in the domain, the BS timer shows the time at which the elected BSR expires.

This system is candidate BSR—Indicates this router is the candidate BSR and provides information on the parameters associated with it.

Example 2. The following example displays information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the FF00::/8 or the default IPv6 multicast range:

```
show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
```

```
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

Example 3. The following example displays information about the C-RP:

```
show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
  Candidate RP: 10::1:1:3
    Priority 192, Holdtime 150
    Advertisement interval 60 seconds
    Next advertisement in 00:00:33
```

59.15 show ipv6 pim counters

To display the Protocol Independent Multicast (PIM) counters, use the **show ipv6 pim counters** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 pim counters

Parameters

N/A.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ipv6 pim counters** command to check if the expected number of PIM protocol messages have been received and sent.

Example

The following example shows the number of PIM protocol messages received and sent:

```
show ipv6 pim counters
iPIM Traffic Counters
Elapsed time since counters cleared: 00:05:29
                       Received    Sent
Valid PIM Packets            22      22
Hello                        22      22
Join-Prune                    0       0
Register                      0       0
Register Stop                 0       0
Assert                        0       0
Bootstrap                     0       0
```

```
Errors:
Send Errors                                0
Bad Checksums                              0
Packets Received on PIM-disabled Interface 0
Packets Received with Unknown PIM Version  0
```

59.16 show ipv6 pim group-map

To display an IPv6 Protocol Independent Multicast (PIM) group mapping table, use the **show ipv6 pim group-map** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 pim group-map [group-*address*]

Parameters

group-address—IPv6 address of the multicast group.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ipv6 pim group-map** command without the *group-address* argument to display information about all groups.

Example

The following example displays information about all groups:

```
show ipv6 pim group-map

Group(s) FF32::/32
  SM RP 20::1:2:1 (?)
  Info source: Local
Group(s) FF33::/32
  SM RP 20::1:1:1 (?)
  Info source: Static
Group(s) FF34::/32
  SM RP 10::1:1:3 (?)
  Info source: From BSR 10.10.0.3 (?), Priority: 192
  Uptime:00:01:26, expires:00:00:34
Group(s) FF35::/32
  SM RP 15::1:1:5 (?)
  Info source: From BSR 10.10.0.5 (mcast1.aaaa.com), Priority: 192
  Uptime:00:00:52, expires:00:00:37
Group(s) FF3E::/32
  SMM
```

```
Group(s) FF7E::1220:2001:DB8::/64
  SM RP 2001:DB8::12 (?)
  Info source: Embedded-RP
```

59.17 show ipv6 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 pim interface [**state-on**] [**state-off**] [*interface-id*]

Parameters

- **state-on**—Displays interfaces with PIM enabled.
- **state-off**—Displays interfaces with PIM disabled.
- **interface-id**—Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ipv6 pim interface** command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

Example

Example 1. The following example displays only PIM state on all interfaces:

```
show ipv6 pim interface
IP Forwarding is enabled
IP Multicast Routing is enabled
rp-embedded: enabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface  Address                   PIM
vlan 1     FE80::208:20FF:FE08:D7FF  off
vlan 100   FE80::208:20FF:FE08:D7FF  on
vlan 102   FE80::208:20FF:FE08:D7FF  on
```

Example 2. The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword when IP Multicast Routing is disabled:

```
show ip pim interface state-on

IP Forwarding is enabled
IP Multicast Routing is disabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface Status    Nbr     Hello    Join-Prune  DR
                    Count   Intvl    Intvl       Prior
vlan 1    disabled
   Address: FE80::208:20FF:FE08:D7FF
   DR:
   Neighbor Filter List: filt
vlan 100  disabled
   Address: FE80::208:20FF:FE08:D7FF
   DR:
   Neighbor Filter List: nbr-filter
vlan 102  enabled
   Address: FE80::208:20FF:FE08:D7FF
   DR:
   Neighbor Filter List:
vlan 103  enabled
   Address:
   DR:
   Neighbor Filter List: filter1
```

Example 3. The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword:

```
show ip pim interface state-on
IP Forwarding is enabled
IP Multicast Routing is enabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface Statuse  Nbr     Hello    Join-Prune  DR
                   Count   Intvl    Intvl       Prior
vlan 100  enabled      0      30      60          1
   Address: FE80::208:20FF:FE08:D7FF
   DR: this system
   Neighbor Filter List: nbr-filter
```

```
vlan 102  enabled      1      30      60          1
   Address: FE80::208:20FF:FE08:D7FF
   DR: FE80::250:E2FF:FE8B:4C80
   Neighbor Filter List:
vlan 103  enabled
   Address:
   DR:
   Neighbor Filter List: filter1
```

Example 4. The following is sample output from the **show ipv6 pim interface** command using the i*nterface-id* argument:

```
show ip pim interface vlan 100
IP Forwarding is enabled
IP Multicast Routing is enabled
SSM IP ranges:
  default
  access list: list1
  access list: list2
Interface Statuse  Nbr     Hello    Join-Prune  DR
                   Count   Intvl    Intvl       Prior
vlan 100  enabled      0      30      60          1
   Address: FE80::208:20FF:FE08:D7FF
   DR: this system
   Neighbor Filter List: nbr-filter
```

59.18 show ipv6 pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by the switch, use the **show ipv6 pim neighbor** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 pim neighbor [**detail**] [*interface-id*]

Parameters

- **detail**—Displays the additional addresses of the neighbors learned, if any, through the Address List (type 24) Hello option.
- **interface-id**—Interface identifier.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ipv6 pim neighbor** command displays which routers on the LAN are configured for PIM.

Example

The following is sample output from the **show ipv6 pim neighbor** command using the detail keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
show ipv6 pim neighbor detail
Neighbor Address(es)     Interface  Uptime   Expires  DR pri
FE80::A8BB:CCFF:FE00:401 vlan 100   01:34:16 00:01:16   1
60::1:1:3
FE80::A8BB:CCFF:FE00:501 vlan 140   01:34:15 00:01:18   1
60::1:1:4
```

59.19 show ipv6 pim rp mapping

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ipv6 pim rp mapping** command in user EXEC or privileged EXEC mode.

Syntax

show ipv6 pim rp mapping [*rp--address*]

Parameters

rp-address—RP IPv6 address. This argument must be in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

Use the **show ipv6 pim rp mapping** command with the *rp-address* argument to display information about the given RP.

Use the **show ipv6 pim rp mapping** command without the *rp-address* argument to display information about all known RPs.

Example

The following example displays information about all known all RPs:

```
show ipv6 pim rp mapping
This system is an RP
Register Acces List: list1
Group(s) FF32::/32
  RP 20::1:2:1 (?)
  Info source: Local
  Uptime: 00:02:40
Group(s) FF33::/32
  RP 20::1:1:1 (?)
  Info source: Static
  Uptime: 00:01:42
Group(s) FF34::/32
  RP 10::1:1:3 (?)
  Info source: From BSR 10.10.0.3 (?), Priority: 192
  Uptime:00:01:26, expires:00:00:34
Group(s) FF35::/32
  RP 15::1:1:5 (?)
  Info source: From BSR 10.10.0.5 (mcast1.aaaa.com), Priority: 192
  Uptime:00:00:52, expires:00:00:37
Group(s) FF7E::1220:2001:DB8::/64
  RP 2001:DB8::12 (?)
  Info source: Embedded-RP
  Uptime:00:00:52
```

60 IGMP/MLD Proxy Commands

60.1 ip igmp-proxy

To add downstream interfaces to an IGMP proxy tree, use the **ip igmp-proxy** command in interface configuration mode. To remove downstream from interfaces to an IGMP proxy tree, use the **no** form of this command.

Syntax

ip igmp-proxy *upstream-interface-id*

no ip igmp-proxy

Parameters

upstream-interface-id—Upstream Interface identifier.

Default Configuration

The protocol is disabled on the interface.

Command Mode

Interface configuration

User Guidelines

Use the **ip igmp-proxy** command to add downstream interfaces to an IGMP proxy tree. If the proxy tree does not exist it is created.

Use the **no** format of the command to remove the downstream interface. When the last downstream interface is removed from the proxy tree it is deleted too.

Example

Example 1. The following example adds a downstream interface to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
interface vlan 100
  ip igmp-proxy vlan 200
exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
interface range vlan 100-105
  ip igmp-proxy vlan 200
exit
```

60.2 ip igmp-proxy downstream protected

To disable forwarding of IP Multicast traffic from downstream interfaces, use the **ip igmp-proxy downstream protected** command in Global configuration mode. To allow forwarding from downstream interfaces, use the **no** form of this command.

Syntax

ip igmp-proxy downstream protected

no p igmp-proxy downstream protected

Parameters

This command has no arguments or keywords.

Default Configuration

Forwarding from downstream interfaces is allowed.

Command Mode

Global configuration mode

User Guidelines

Use the **ip igmp-proxy downstream protected** command to block forwarding from downstream interfaces.

Example

The following example prohibits forwarding from downstream interfaces:

```
p igmp-proxy downstream protected
```

60.3 ipv6 mld-proxy

To add downstream interfaces to a MLD proxy tree, use the **ip mld-proxy** command in interface configuration mode. To remove downstream from interfaces to a MLD proxy tree, use the **no** form of this command.

Syntax

ipv6 mld-proxy *upstream-interface-id*

no ipv6 mld-proxy

Parameters

upstream-interface-id—Upstream Interface identifier.

Default Configuration

The protocol is disabled on the interface.

Command Mode

Interface configuration

User Guidelines

Use the **ipv6 mld-proxy** command to add a downstream interface to a MLD proxy tree. If the proxy tree does not exist it is created.

Use the **no** format of the command to remove the downstream interface. When the last downstream interface is removed from the proxy tree it is deleted too.

Example

Example 1. The following example adds a downstream interface to a MLD Proxy process with vlan 200 as its Upstream interface:

```
interface vlan 100
  ipv6 mld-proxy vlan 200
exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
interface range vlan 100-105
  ipv6 mld-proxy vlan 200
exit
```

60.4 ipv6 mld-proxy downstream protected

To disable forwarding of IPv6 Multicast traffic from downstream interfaces, use the i**pv6 mld-proxy downstream protected** command in Global configuration mode. To allow forwarding from downstream interfaces, use the **no** form of this command.

Syntax

ipv6 mld-proxy downstream protected

no ipv6 mld-proxy downstream protected

Parameters

This command has no arguments or keywords.

Default Configuration

Forwarding from downstream interfaces is allowed.

Command Mode

Global configuration mode

User Guidelines

Use the **pv6 mld-proxy downstream protected** command to block forwarding from downstream interfaces.

Example

The following example prohibits forwarding from downstream interfaces:

ipv6 mld-proxy downstream protected

60.5 show ip igmp-proxy interface

To display information about interfaces configured for IGMP Proxy, use the **show ip igmp-proxy interface** command in EXEC or privileged EXEC mode.

Syntax

show ip igmp-proxy interface [*interface-id*]

Parameters

interface-id—Display IGMP Proxy information about the interface.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ip igmp-proxy interface** command is used to display all interfaces where the IGMP Proxy is enabled or to display the IGMP Proxy configuration for a given interface.

Example

Example 1. The following example displays IGMP Proxy status on all interfaces where the IGMP Proxy is enabled:

```
show ip igmp-proxy interface

* - the switch is the Querier on the interface


IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
IP Multicast Tarffic is discarded from Downstream interfaces
Interface  Type
 vlan 100  upstream
*vlan 102  downstream
*vlan 110  downstream
 vlan 113  downstream
```

Example 2. The following is sample output from the **show ip igmp-proxy interface** command for given upstream interface:

```
show ip igmp-proxy interface vlan 100


* - the switch is the Querier on the interface
```

```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
IP Multicast Tarffic is discarded from Downdtream interfaces
vlan 100 is a Upstream interface
Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the **show ip igmp-proxy interface** command for given downstream interface:

```
show ip igmp-proxy interface vlan 102


IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
IP Multicast Tarffic is allowed from Downdtream interfaces
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Upstream interface: vlan 100
```

Example 4. The following is sample output from the **show ip igmp-proxy interface** command for an interface on which IGMP Proxy is disabled:

```
show ip igmp-proxy interface vlan 1


IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is disabled
```

60.6 show ipv6 mld-proxy interface

To display information about interfaces configured for MLD Proxy, use the **show ipv6 mld-proxy interface** command in EXEC or privileged EXEC mode.

Syntax

show ipv6 mld-proxy interface [*interface-id*]

Parameters

interface-id—Display MLD Proxy information about the interface.

Command Mode

User EXEC

Privileged EXEC

User Guidelines

The **show ipv6 mld-proxy interface** command is used to to display all interfaces where the MLD Proxy is enabled or to display the MLD Proxy configuration for a given interface.

Example

Example 1. The following example displays MLD Proxy status on all interfaces where the MLD Proxy is enabled:

```
show ip mld-proxy interface

* - the switch is the Querier on the interface

IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
IPv6 Multicast Tarffic is discarded from Downdtream interfaces
Interface  Type
 vlan 100  upstream
*vlan 102  downstream
*vlan 110  downstream
 vlan 113  downstream
```

Example 2. The following is sample output from the **show ipv6 mld-proxy interface** command for given upstream interface:

```
show ipv6 mld-proxy interface vlan 100

* - the switch is the Querier on the interface

IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
IPv6 Multicast Tarffic is discarded from Downdtream interfaces
vlan 100 is a Upstream interface
Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the **show ipv6 mld-proxy interface** command for given downstream interface:

```
show ipv6 mld-proxy interface vlan 102

IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
```

```
MLD Proxy is enabled
IPv6 Multicast Tarffic is allowed from Downdtream interfaces
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Upstream interface: vlan 100
```

Example 4. The following is sample output from the **show ipv6 mld-proxy interface** command for an interface on which IGMP Proxy is disabled:

```
show ipv6 mld-proxy interface vlan 1


IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is disabled
```

61 DNS Client Commands

61.1 clear host

Use the **clear host** command in privileged EXEC mode to delete dynamic hostname-to-address mapping entries from the DNS client name-to-address cache.

Syntax

clear host {*hostname* | *****}

Parameters

- **hostname**—Name of the host for which hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.
- /*—Specifies that all the dynamic hostname-to-address mappings are to be deleted from the DNS client name-to-address cache.

Default Configuration

No hostname-to-address mapping entries are deleted from the DNS client name-to-address cache.

Command Mode

Privileged EXEC mode

User Guidelines

To remove the dynamic entry that provides mapping information for a single hostname, use the *hostname* argument. To remove all the dynamic entries, use the ***** keyword.

To define a static hostname-to-address mappings in the DNS hostname cache, use the ip host command.

To delete a static hostname-to-address mappings in the DNS hostname cache, use the **no** ip host command.

Example

The following example deletes all dynamic entries from the DNS client name-to-address cache.

```
clear host *
```

61.2 ip domain lookup

Use the **ip domain lookup** command in Global Configuration mode to enable the IP Domain Naming System (DNS)-based host name-to-address translation.

To disable the DNS, use the **no** form of this command.

Syntax

ip domain lookup

no ip domain lookup

Parameters

N/A

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
```

61.3 ip domain name

Use the **ip domain name** command in Global Configuration mode. to define a default domain name that the switch uses to complete unqualified hostnames (names without a dotted-decimal domain name).

To delete the static defined default domain name, use the **no** form of this command.

Syntax

ip domain name *name*

no ip domain name

Parameters

name—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

No default domain name is defined.

Command Mode

Global Configuration mode

User Guidelines

Any IP hostname that does not contain a domain name (that is, any name without a dot) will have the dot and the default domain name appended to it before being added to the host table.

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 website.com
```

61.4 ip domain polling-interval

Use the **ip domain polling-interval** command in Global Configuration mode to specify the polling interval.

Use the **no** form of this command to return to the default behavior.

Syntax

ip domain polling-interval *seconds*

no ip domain polling-interval

Parameters

seconds—Polling interval in seconds. The range is from (2*(R+1)*T) to 3600.

Default Configuration

The default value is 2 * (R+1) * T, where

R is a value configured by the **ip domain retry** command.

T is a value configured by the **ip domain timeout** command.

Command Mode

Global Configuration mode

User Guidelines

Some applications communicate with the given IP address continuously. DNS clients for such applications, which have not received resolution of the IP address or have not detected a DNS server using a fixed number of retransmissions, return an error to the application and continue to send DNS Request messages for the IP address using the polling interval.

Example

The following example shows how to configure the polling interval of 100 seconds:

```
ip domain polling-interval 100
```

61.5 ip domain retry

Use the **ip domain retry** command in Global Configuration mode to specify the number of times the device will send Domain Name System (DNS) queries when there is no replay.

To return to the default behavior, use the **no** form of this command.

Syntax

ip domain retry *number*

no ip domain retry

Parameters

number—Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 16.

Default Configuration

The default value is 2.

Command Mode

Global Configuration mode

User Guidelines

The number argument specifies how many times the DNS query will be sent to a DNS server until the switch decides that the DNS server does not exist.

Example

The following example shows how to configure the switch to send out 10 DNS queries before giving up:

```
ip domain retry 10
```

61.6 ip domain timeout

Use the **ip domain timeout** command in Global Configuration mode to specify the amount of time to wait for a response to a DNS query.

To return to the default behavior, use the **no** form of this command.

Syntax

ip domain timeout *seconds*

no ip domain timeout

Parameters

seconds—Time, in seconds, to wait for a response to a DNS query. The range is from 1 to 60.

Default Configuration

The default value is 3 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use the command to change the default time out value. Use the **no** form of this command to return to the default time out value.

Example

The following example shows how to configure the switch to wait 50 seconds for a response to a DNS query:

```
ip domain timeout 50
```

61.7 ip host

Use the **ip host** Global Configuration mode command to define the static host name-to-address mapping in the DNS host name cache.

Use the **no** form of this command to remove the static host name-to-address mapping.

Syntax

ip host *hostname address1* [*address2...address8*]

no ip host *name* **ip host** *name* [*address1...address8*]

Parameters

- **hostname**—Name of the host. (Length: 1–158 characters. Maximum label length of each domain level is 63 characters).
- **address1**—Associated host IP address (IPv4 or IPv6, if IPv6 stack is supported).
- **address2...address8**—Up to seven additional associated IP addresses, delimited by a single space (IPv4 or IPv6, if IPv6 stack is supported).

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.

An IP application will receive the IP addresses in the following order:

1. IPv6 addresses in the order specified by the command.
2. IPv4 addresses in the order specified by the command.

Use the **no** format of the command with the *address1...address8* argument to delete the specified addresses. The entry is deleted if all its addresses are deleted.

Example

The following example defines a static host name-to-address mapping in the host cache.

```
ip host accounting.website.com 176.10.23.1
```

61.8 ip name-server

Use the **ip name-server** command in Global Configuration mode to specify the address of one or more name servers to use for name and address resolution.

Use the **no** form of this command to remove the static specified addresses.

Syntax

ip name-server *server1-address* [*server-address2...erver-address8*]

no ip name-server [*server-address1*...*server-address8*]

Parameters

- **server-address1**—IPv4 or IPv6 addresses of a single name server.
- **server-address2...server-address8**—IPv4 or IPv6 addresses of additional name servers.

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.

Each **ip name-server** command replaces the configuration defined by the previous one (if one existed).

Example

The following example shows how to specify IPv4 hosts 172.16.1.111, 172.16.1.2, and IPv6 host 2001:0DB8::3 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

61.9 show hosts

Use the **show hosts** command in privileged EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

Syntax

show hosts [**all** | *hostname*]

Parameters

- **all**—The specified host name cache information is to be displayed for all configured DNS views. This is the default.
- **hostname**—The specified host name cache information displayed is to be limited to entries for a particular host name.

Command Mode

Privileged EXEC

Default Configuration

Default is **all**.

User Guidelines

This command displays the default domain name, a list of name server hosts, and the cached list of host names and addresses.

Example

The following is sample output with no parameters specified:

```
show hosts
Name/address lookup is enabled
Domain Timeout: 3 seconds
Domain Retry: 4 times
Domain Polling Interval: 10 seconds

Default Domain Table
Source  Interface Preference Domain
static                       website.com
dhcpv6  vlan 100      1      qqtca.com
dhcpv6  vlan 100      2      company.com
dhcpv6  vlan 1100     1      pptca.com

Name Server Table
Source  Interface Preference  IP Address
static               1        192.0.2.204
static               2        192.0.2.205
static               3        192.0.2.105
DHCPv6      vlan 100 1        2002:0:22AC::11:231A:0BB4
DHCPv4      vlan 1   1        192.1.122.20
DHCPv4      vlan 1   2        154.1.122.20

Casche Table
Flags: (static/dynamic, OK/Ne/??)
OK - Okay, Ne - Negative Cache, ?? - No Response
Host Flag Address;Age...in preference order

example1.company.com (dynamic, OK) 2002:0:130F::0A0:1504:0BB4;1
112.0.2.10 176.16.8.8;123 124 173.0.2.30;39
example2.company.com (dynamic, ??)
example3.company.com (static, OK) 120.0.2.27
example4.company.com (dynamic, OK) 24 173.0.2.30;15
example5.company.com (dynamic, Ne); 12
```