

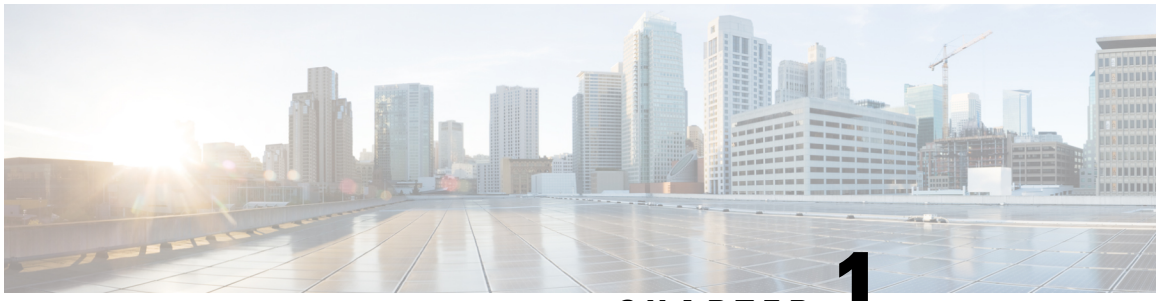
Cisco Catalyst C1300X CLI Guide Version 4.10.0.xx

First Published: 2025-10-01

Last Modified: 2025-10-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2025 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Introduction

This chapter contains the following sections:

- Overview, on page 1
- User Privilege Levels, on page 1
- CLI Command Modes, on page 2
- Interfaces for Debug Access, on page 4
- Accessing the CLI, on page 5
- CLI Command Conventions, on page 6
- Editing Features, on page 7
- Interface Naming Conventions, on page 9
- IPv6z Address Conventions, on page 11
- Loopback Interface, on page 11
- Managing Ports Via CLI, on page 12
- Remote IP Address and OOB Port, on page 13
- PHY Diagnostics, on page 13
- CLI Output Modifiers, on page 13

Overview

The CLI is divided into various command modes. Each mode includes a group of commands.

These modes are described in CLI Command Modes, on page 2.

Users are assigned privilege levels. Each user privilege level can access specific CLI modes.

User levels are described in the section below.

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 7—Users with this level can run commands in the User EXEC mode and a subset of commands in the Privileged EXEC mode. Users at this level cannot access the web GUI.

- 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 lower level user to temporarily become a higher level user. For example, the user may go from level 1 to level 7, level 1 to 15, or level 7 to level 15.

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 7 or 15. You can go from level 1 to level 7 or directly to 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.

Example—Create passwords for level 7 and 15 (by the administrator):

```
switchxxxxxx#configure
switchxxxxxx<conf># enable password level 7 level7@aBc
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>
```

Example 2— 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#
```



Note If authentication of passwords is performed on RADIUS or TACACS+ servers, the passwords assigned to user level 7 and user level 15 must be configured on the external server and associated with the $enable7$ and $enable15$ user names, respectively.

CLI Command Modes

The CLI is divided into four command modes. The command modes are (in the order in which they are accessed):

- User EXEC mode
- Privileged EXEC mode
- Global Configuration mode

Each command mode has its own unique console prompt and set of CLI commands. Entering a question mark at the console prompt displays a list of available commands for the current mode and for the level of the user. Specific commands are used to switch from one mode to another.

Users are assigned privilege levels that determine the modes and commands available to them.

User EXEC Mode

Users with level 1 initially log into User EXEC mode. User EXEC mode is used for tasks that do not change the configuration, such as performing basic tests and listing system information.

The user-level prompt consists of the switch host name followed by a #. The default host name is switchxxxxxx where xxxxxx is the last six digits of the device's MAC address, as shown below

switchxxxxxx#

The default host name can be changed via the hostname command in Global Configuration mode.

Privileged EXEC Mode

A user with level 7 or 15 automatically logs into Privileged EXEC mode.

Users with level 1 can enter Privileged Exec mode by entering the enable command, and when prompted, the password for level 15.

To return from the Privileged EXEC mode to the User EXEC mode, use the disable command

Global Configuration Mode

The Global Configuration mode is used to run commands that configure features at the system level, as opposed to the interface level.

Only users with command level of 7 or 15 can access this mode.

To access Global Configuration mode from Privileged EXEC mode, enter the configure command at the Privileged EXEC mode prompt and press Enter. The Global Configuration mode prompt, consisting of the device host name followed by (config)#, is displayed:

switchxxxxxx(config)#

Use any of the following commands to return from Global Configuration mode to the Privileged EXEC mode:

- exit
- end
- Ctrl+Z

The following example shows how to access Global Configuration mode and return to Privileged EXEC mode:

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

Interface or Line Configuration Modes

Various submodes may be entered from Global Configuration mode. These submodes enable

performing commands on a group of interfaces or lines.

For instance to perform several operations on a specific port or range of ports, you can enter

the Interface Configuration mode for that interface.

The following example enters Interface Configuration mode for vlan1 and then sets their

speed:

The exit command returns to Global Configuration mode.

```
switchxxxxxx#
switchxxxxxx# configure
switchxxxxxx(config)# interface range vlan1
switchxxxxxx(config-if)#speed 10
switchxxxxxx(config-if)#exit
switchxxxxxx(config)#
```

The following is a sample of some of the available submodes:

- Interface—Contains commands that configure a specific interface (port, VLAN, port channel, or tunnel) or range of interfaces. The Global Configuration mode command interface is used to enter the Interface Configuration mode. The interface Global Configuration command is used to enter this mode.
- Line Interface—Contains commands used to configure the management connections for the console, Telnet and SSH. These include commands such as line timeout settings, etc. The line Global Configuration command is used to enter the Line Configuration command mode.
- VLAN Database—Contains commands used to configure a VLAN as a whole. The vlan database Global Configuration mode command is used to enter the VLAN Database Interface Configuration mode.
- Management Access List—Contains commands used to define management access-lists. The management access-list Global Configuration mode command is used to enter the Management Access List Configuration mode.
- MAC Access-List, IPv6 Access List, IP Access List—Configures conditions required to allow traffic based on MAC addresses, IPv6 address and IPv4 address, respectively. The mac access-list, ipv6 access-list and ip access-list Global Configuration mode commands are used to enter the these configuration mode.

To return from any Interface Configuration mode to the Global Configuration mode, use the exit command.

Interfaces for Debug Access

In addition to the standard CLI interface modes detailed above, the device supports additional interfaces for device debug access. These interlaces are intended to be used by a Cisco Support Team personnel, in cases where it is required to debug device's behavior. These interfaces are password protected.

The device supports the following debug interfaces:

- U-BOOT access during boot sequence (access is possible only via serial console terminal)
- Linux Kernel access during boot sequence (access is possible only via serial console terminal)
- Run time debug modes - allows Cisco Support Team personnel to view device settings, and to apply protocol and layer 1 debug commands and settings (access is possible via serial, telnet or SSH console terminal)

The password for these interfaces is generated as follows:

- Upon access to debug interface the device generates a random hash value and displays it on the screen.
- The hash value is sent by the device administrator and the Cisco support person for signing on a secure Cisco server using a private key.
- The output of this operation is used as the password for debug interface access.
- The password is good for current session. On the next attempt to enter a debug interface, or following a device reboot the device will generate a new random hash.

Accessing the CLI

The CLI can be accessed from a terminal or computer by performing one of the following tasks:

- Running a terminal application, such as HyperTerminal, on a computer's com port that is directly connected to the switch's console port,

  or

- Running a Telnet session from a command prompt on a computer with a network connection to the switch.
- Using SSH from an application that supports SSH client running on a computer with a network connection to the switch.



Note Telnet and SSH are disabled by default on the switch.

If access is via a Telnet or SSH connection, ensure that the following conditions are met before using CLI commands:

- The switch has a defined IP address
- Corresponding management access is enabled.
- There is an IP path such that the computer and the switch can reach each other

Using a Terminal over the Console Interface

The device supports a dual console management interface - a Type-C USB interface and an RJ45 port. If both Type-C USB and RJ45 are connected the Type-C USB interface has precedence. To support the Type-C interface a driver may need to be installed on the management station.



Note The Type-C USB interface will become active a few seconds after the device is turned on/rebooted.

After the computer and switch are connected, run a terminal application to access the CLI. The terminal emulator must be configured to databits=8 and parity=none.

Click **Enter** twice, so that the device sets the serial port speed to match the PC's serial port speed.

When the CLI appears, enter cisco at the User Name prompt and then enter cisco for the Password prompt.



Note If this is the first time that you have logged on with the default username and password, the device will display a prompt to change username and Password. The new password needs to comply to password complexity rules.

The switchxxxxxx# prompt is displayed.

You can now enter CLI commands to manage the switch. For detailed information on CLI commands, refer to the appropriate chapter(s) of this reference guide.

Using Telnet over an Ethernet Interface

Telnet provides a method of connecting to the CLI over an IP network.

To establish a telnet session from the command prompt, perform the following steps

Procedure

Step 1 Click **Start,** then select **All Programs > Accessories > Command Prompt** to open a command prompt.

Step 2 At the prompt, enter **telnet 1<IP address of switch**>, then press **Enter**.

Step 3 CLI will be displayed.

Step 4 When the CLI appears, enter the defined username at the User Name prompt and then enter the defined password at the Password prompt.

Note
If this is the first time that you have logged on with the default username and password, the device will display a prompt to change username and Password. The new password needs to comply to password complexity rules.

The switchxxxxxx# prompt is displayed. You can now enter CLI commands to manage the switch. For detailed information on CLI commands, refer to the appropriate chapter(s) of this reference guide.

CLI Command Conventions

When entering commands there are certain command entry standards that apply to all commands. The following table describes the command conventions.

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry.
{ }	In a command line, curly brackets indicate a selection of compulsory parameters separated 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

Convention	Description
"" (inverted commas)	When the input string contains space and/or reserved words (i.e. VLAN), put the string in inverted commas.
parameter	Italic text indicates a parameter.
press key	Names of keys to be pressed are shown in bold.
Ctrl+F4	Keys separated by the + character are to be pressed simultaneously on the keyboard
Screen Display	Fixed-width font indicates CLI prompts, CLI commands entered by the user, and system messages displayed 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.
text	When free text can be entered as a parameter for a command (for example in command: snmp-server contact) if the text consists of multiple words separated by blanks, the entire string must appear in double quotes. For example: **snmp-server contact** "QA on floor 8"

Editing Features

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 Gigabitethernet 1, show, interfaces and status are keywords, Gigabitethernet is an argument that specifies the interface type, and1 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:

switchxxxxxx(config)# username admin password Alansmith1

When working with the CLI, the command options are not displayed. The standard command to request help is ?

There are two instances where help information can be displayed:

- Keyword lookup—The character ? is entered in place of a command. A list of all valid commands and corresponding help messages are is displayed
- Partial keyword lookup—If a command is incomplete and or the character ? is entered in place of a parameter, the matched keyword or parameters for this command are displayed.

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.

Keyword	Description
Up-Arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-Arrow key	Returns to more recent commands in the history buffer after recalling commands with the up-arrow key. Repeating the key sequence will recall successively more recent commands.

By default, the history buffer system is enabled, but it can be disabled at any time. For more information on enabling or disabling the history buffer, refer to 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 216. By configuring 0, the effect is the same as disabling the history buffer system. For more information on configuring the command history buffer, refer to the **history size** command.

To display the history buffer, refer to the **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 Reference Guide provides a description of the negation effect for each CLI command.

Command Completion

If the command entered is incomplete, invalid or has missing or invalid parameters, then the appropriate error message is displayed. This assists in entering the correct command. By pressing Tab after an incomplete command is entered, the system will attempt to identify and complete the command. 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.

Keyboard Shortcuts

The CLI has a range of keyboard shortcuts to assist in editing the CLI commands. The following table describes the CLI shortcuts.

Keyboard Key	Description
Up-arrow	Recalls commands from the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down-arrow	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.

Keyboard Key	Description
Ctrl+Z / End	Returns back to the Privileged EXEC mode from any configuration mode.
Backspace	Deletes one character left to the cursor position.

Copying and Pasting Text

Up to 1000 lines of text (or commands) can be copied and pasted into the device.



Note It is the user's responsibility to ensure that the text copied into the device consists of legal commands only.

When copying and pasting commands from a configuration file, make sure that the following conditions exist:

- A device Configuration mode has been accessed.

The commands contain no encrypted data, like encrypted passwords or keys. Encrypted data cannot be copied and pasted into the device except for encrypted passwords where the keyword encrypted is used before the encrypted data (for instance in the enable password command).

Interface Naming Conventions

Interfaces on the device can be one of the following types:

- Gigabit Ethernet (10/100/1000 kbits) ports—These can be written as either GigabitEthernet or gi or GE.
- 2.5 Gigabit Ethernet (10/100/1000/25000 kbits) ports—These can be written as either TwoPointFiveGigabitEthernet or tw.
- 5 Gigabit Ethernet (10/100/1000/25000/50000 kbits) ports—These can be written as either FiveGigabitEthernet or fi.
- LAG (Port Channel)—Written as either Port-Channel or po.
- VLAN—Written as VLAN
- Tunnel—Written as tunnel or tu
- OOB—Written as OutOfBand or oob

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

- Type of Interface—As described above
- Unit Number—Unit in stack.
- Slot Number—The slot number is always 0.
- The syntax for interface names in stacking mode is:

  {<port-type>[ ][<unit-number>/]<slot-number>/<port-number>} | {port-channel | po |

  }[ ]<port-channel-number> |

{tunnel | tu}[ ]<tunnel-number> | vlan[ ]<vlan-id>

- Interface Number—Port, LAG, tunnel or VLAN numbers

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

```
switchxxxxxx(config)#interface GigabitEthernet 1
switchxxxxxx(config)#interface GE 1
switchxxxxxx(config)#interface TwoPointFiveGigabitEthernet
switchxxxxxx(config)#interface po1
switchxxxxxx(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:

```
switchxxxxxx#configure
switchxxxxxx(config-if)#interface range gi1-5g
```

List of Multiple Interface Types

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:

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

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.

Loopback Interface

When an IP application on a router wants to communicate with a remote IP application, it must select the local IP address to be used as its IP address. It can use any IP address defined on the router, but if this link goes down, the communication is aborted, even though there might well be another IP route between these IP applications.

The loopback interface is a virtual interface whose operational state is always up. If the IP address that is configured on this virtual interface is used as the local address when communicating with remote IP applications, the communication will not be aborted even if the actual route to the remote application was changed.

The name of the loopback interface is loopback1.

A loopback interface does not support bridging; it cannot be a member of any VLAN, and no layer 2 protocol can be enabled on it.

Layer 3 Specification

IP Interface

IPv4 and IPv6 addresses can be assigned to a loopback interface.

The IPv6 link-local interface identifier is 1.

Routing Protocols

A routing protocol running on the switch supports the advertising of the IP prefixes defined on the loopback interfaces via the routing protocol redistribution mechanism.

Configuration Examples

Static Routing

The following example shows you how to configure IP on a switch with static routing:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.10.10.2 /24
Switch(config-if)# ipv6 address 2001:DB8:2222:7270::2312/64
Switch(config-if)# exit
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.11.11.2 /24
Switch(config-if)# ipv6 address 2001:DB8:3333:7271::2312/64
Switch(config-if)# exit
Switch(config)# interface loopback 1
Switch(config-if)# ip address 172.25.13.2 /32
Switch(config-if)# ipv6 address 2001:DB8:2222:7272::72/128
Switch(config-if)# exit
Switch(config)# ip route 0.0.0.0/0 10.10.11.1
Switch(config)# ip route 10.11.0.0 /16 10.11.11.1
Switch(config)# ipv6 route 0::/0 2001:DB8:2222:7270::1
Switch(config)# ipv6 route 2001:DB8:3333::/48
2001:DB8:3333:7271::1
```

The neighbor router 10.10.11.1 should be configured with the following static route: ip route 172.25.13.2 /32 10.10.10.2.

The neighbor router 10.11.11.1 should be configured with the following static route: ip route 172.25.13.2 /32 10.11.11.2.

The neighbor router 2001:DB8:2222:7270::1 connected to VLAN 1 should be configured with the following static route:

ipv6 route 2001:DB8:2222:7272::72/128 2001:DB8:2222:7270::2312

The neighbor router 2001:DB8:3333:7271::1 connected to VLAN 1 should be configured with the static route defined immediately below.

IPv6 Route 2001:DB8:2222:7272::72/128 2001:DB8:3333:7271::2312

Managing Ports Via CLI

To access a port interface on units that support stacking, type “interfaceGigabitEthernetX/0/Z (for 1gig interfaces), or “interface TenGigabitEthernetX/0/Y for 10gig ports with X (1-4) being the stack ID, Y for the uplink ports number (1-4), and Z for the downlink port number; Z is between 1- 48 even for the units that have less than 48 ports.

Fiber cable and Transceivers

Cisco brand provides a panoply a SFP modules, while our switches support other 3rd party, it is important to pay attention on the type of fiber cable to use in conjunction with the specific SFP module.

Fiber cables can be classified in two types: Single Mode and Multimode. The main difference is the distance they are capable of covering and their diameter. Single Mode fibers cover greater distance compared to Multimode and has lower diameter (around 9 micrometer) while the Multimode fibers diameter is 50-62.5 micrometer.

DAC cables for Direct Attach Copper Cable, on the other hand, can be used for short distances. They are mainly based on the Multimode-Standard type of transceivers due to the fact that the max distance they can cover is 15m. The AOC (Active Optical Cable), however, is a different story.

When troubleshooting fiber connectivity related issues, it is important to make a distinction between SMF (Single Mode Fiber cables), and MMF (Multimode Fiber cables) and their corresponding SFP transceivers a given fiber can support.

Cisco has matrix that we can refer to when trying to make a determination of the correct pairing. The following link provide some insight on Cisco 10gig SFP

Example:

The Cisco SFP-10G-SR only works with MMF type of cable of 62.5 micrometer diameter, while the Cisco SFP-10G-LR works only with SMF type of cable. The MMF range from OM1-OM5. OM is for Optical Multimode. OM1 type cables have a diameter of 62.5 micrometer, while all other types (OM2-OM5) have a diameter of 50 micrometer.

So, it is important to know what is being done to avoid mixing them up.

Remote IP Address and OOB 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 requires specific route table configuration

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.

PHY Diagnostics

The following exceptions exist:

- Copper Ports—PHY diagnostics are only supported on copper ports.
- 10G ports—TDR test is supported when the operational port speed is 10G. Cable length resolution is 20 meters.

CLI Output Modifiers

To all **show** and **more** commands (except **show technical support**) an output modifier may be added as follows:

```
<show/more command> | <output-modifier> <regular-expression-pattern>
```

The output modifiers are:

- **begin:** Start output from the first line that has a sequence of characters matching thegiven regular expression pattern
- **include:** Includes only lines that have a sequence of characters matching the given regular expression pattern.
- **exclude:** Excludes all lines that have a sequence of characters matching the given regular expression pattern.
- **count:** Counts all lines that have a sequence of characters matching the given regular expression pattern and displays the result (no other output is displayed).

Note Only 1 output modifier can be used in each command. The remainder of the text typed in is part of the regular expression pattern.

A regular expression is a pattern (a phrase, number, or more complex pattern). The CLI String Search feature matches regular expressions to the show or more command output. Regular expressions are case-sensitive and allow for complex matching requirements.

A regular expression can be a single-character pattern or a multiple-character pattern. That is, a regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. The pattern in the command output is referred to as a string. This section describes creating both single-character patterns and multiple-character patterns. It also discusses creating more complex regular expressions, using multipliers, alternation, anchoring, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or ~) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. The following table lists the keyboard characters that have special meanings

Character	Meaning
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
^	Matches the beginning of the string.
$	Matches the end of the string.

To use these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\).

The following examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively.

\$ _ \+

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. Only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([ ]). For example, [aeiou] matches any one of the five vowels of the lowercase alphabet, while [abcdABCD] matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the endpoints of the range separated by a dash (-).

Simplify the previous range as follows:

[a-dA-D]

To add a dash as a single-character pattern in your range, include another dash and precede it with a backslash:

[a-dA-D\-]

You can also include a right square bracket (]) as a single-character pattern in your range, as shown here:

[a-dA-D\-\]]

The previous example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket. You can reverse the matching of the range by including a caret (^) at the start of the range. The following example matches any letter except the ones listed:

[^a-dqsv]

The following example matches anything except a right square bracket (]) or the letter d:

[^\]d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, in that order, pattern matching fails. The multiple-character regular expression a. uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of the period character by inserting a backslash before it. For example, when the expression a\. is used in the command syntax, only the string a. will be matched.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. For example, telebit 3107 v32bis is a valid regular expression.

Multipliers

You can create more complex regular expressions that instruct the system to match multiple occurrences of a specified regular expression. To do so, use some special characters with your single-character and multiple-character patterns. Table 1 lists the special characters that specify multiples of a regular expression.

Table 1: Table 1: Special Characters Used as Multipliers

Character	Description
*	Matches 0 or more single-character or multiple-character patterns.
+	Matches 1 or more single-character or multiple-character patterns.
?	Matches 0 or 1 occurrences of a single-character or multiple-character pattern.

The following example matches any number of occurrences of the letter a, including none:

a*

The following pattern requires that at least one letter a be in the string to be matched:

a+

The following pattern matches the string bb or bab:

ba?b

The following string matches any number of asterisks (*):

**

To use multipliers with multiple-character patterns, enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

The following pattern matches one or more instances of alphanumeric pairs, but not none (that is, an empty string is not a match):

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression above matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Only one of the alternatives can match the string. For example, the regular expression codex|telebit either matches the string codex or the string telebit, but not both codex and telebit.

Anchoring

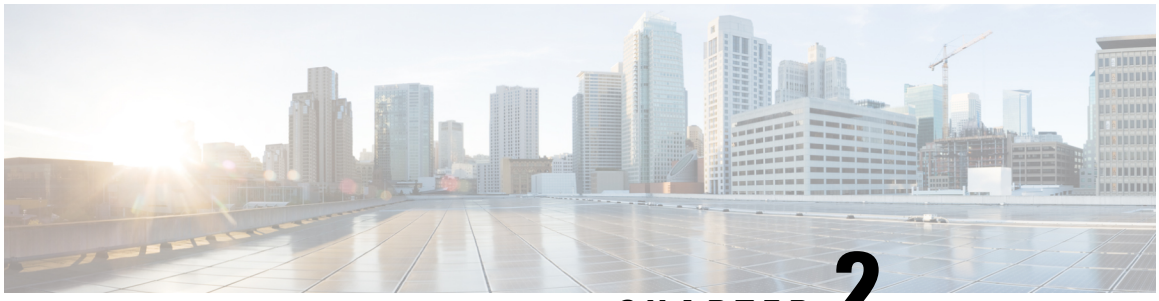
You can instruct the system to match a regular expression pattern against the beginning or the end of the string. You anchor these regular expressions to a portion of the string using the special characters shown in Table 2.

Table 2: Table 2: Special Characters Used for Anchoring

Character	Description
^	Matches the beginning of the string.
$	Matches the end of the string.

For example, the regular expression ^con matches any string that starts with con, and $sole matches any string that ends with sole.

In addition to indicating the beginning of a string, the ^ symbol can be used to indicate the logical function not when used in a bracketed range. For example, the expression [^abcd] indicates a range that matches any single letter, as long as it is not the letters a, b, c, or d.



CHAPTER 2

802-1x Commands

This chapter contains the following sections:

- aaa authentication dot1x, on page 18
- authentication open, on page 19
- clear dot1x statistics, on page 19
- data , on page 20
- description 802.1x , on page 21
- dot1x auth-not-req, on page 21
- dot1x authentication, on page 22
- dot1x credentials, on page 23
- dot1x eap-max-retrans, on page 24
- dot1x guest-vlan, on page 24
- dot1x guest-vlan enable, on page 25
- dot1x guest-vlan timeout, on page 26
- dot1x host-mode, on page 27
- dot1x mac-auth, on page 29
- dot1x mac-auth password, on page 30
- dot1x max-hosts, on page 31
- dot1x max-login-attempts, on page 32
- dot1x max-req, on page 33
- dot1x page customization, on page 33
- dot1x port-control, on page 34
- dot1x radius-attributes vlan, on page 35
- dot1x re-authenticate, on page 37
- dot1x reauthentication, on page 37
- dot1x supplicant, on page 38
- dot1x supplicant traps authentication failure, on page 39
- dot1x supplicant traps authentication success, on page 39
- dot1x system-auth-control, on page 40
- dot1x timeout eap-timeout, on page 40
- dot1x timeout quiet-period, on page 41
- dot1x timeout reauth-period, on page 42
- dot1x timeout server-timeout, on page 43
- dot1x timeout silence-period, on page 43

- dot1x timeout supp-timeout, on page 44
- dot1x timeout supplicant-held-period, on page 45
- dot1x timeout tx-period, on page 46
- dot1x traps authentication failure, on page 46
- dot1x traps authentication quiet, on page 47
- dot1x traps authentication success, on page 48
- dot1x unlock client, on page 48
- dot1x violation-mode, on page 49
- password , on page 50
- show dot1x, on page 51
- show dot1x credentials, on page 55
- show dot1x locked clients, on page 55
- show dot1x sessions interface, on page 56
- show dot1x statistics, on page 57
- show dot1x users, on page 59
- username (dot1x credentials), on page 60

aaa authentication dot1x

To specify which servers are used for authentication when 802.1X authentication is enabled, use the **aaa authentication dot1x** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

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. Even if no response was received, authentication succeeds.

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

authentication open

To enable open access (monitoring mode) on this port, use the **authentication open** command in Interface Configuration mode. To disable open access on this port, use the **no** form of this command.

Syntax

authentication open

no authentication open

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

Open Access or Monitoring mode allows clients or devices to gain network access before authentication is performed. In the mode the switch performs failure replies received from a Radius server as success.

Example

The following example enables open mode on interface gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# authentication open
```

clear dot1x statistics

To clear 802.1X statistics, use the **clear dot1x statistics** command in Privileged EXEC mode.

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 mode

User Guidelines

This command clears all the counters displayed in the **show dot1x** and **show dot1x statistics** command.

Example

```
switchxxxxxx# clear dot1x statistics
```

data

To specify web-based page customizing, the **data** command is used in Web-Based Page Customization Configuration mode.

Syntax

data *value*

Parameters

- ***value***—String of hexadecimal digit characters up to 320 characters.

Default Configuration

No user customization.

Command Mode

Web-Based Page Customization Configuration mode

User Guidelines

The command should not be entered or edited manually (unless using copy-paste). It is a part of the configuration file produced by the switch.

A user can only customize the web-based authentication pages by using the WEB interface.

Example 1—The following example shows a partial web-based page customization configuration:

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

Example 2—The following example shows how Web-Based Page customization is displayed when running the **show running-config** command:

```
switchxxxxxx# show running-config
dot1x page customization
data ********
exit
```

description 802.1x

To specify a description for an 802.1X credential structure, use the **description** command in Dot1x credentials configuration mode. To remove the description, use the **no** form of this command.

Syntax

description *text*

no description

Parameters

- ***text***—Text description. The description can be up to 80 characters.

Default Configuration

A description is not specified.

Command Mode

Dot1x credentials configuration mode

User Guidelines

An 802.1X credential structure is necessary when configuring the switch as a supplicant (client). This credentials structure must contain a username and password and may contain a description.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 6f3c576n8
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connected to site-A
```

dot1x auth-not-req

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

Syntax

dot1x auth-not-req

no dot1x auth-not-req

Default Configuration

Access is enabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

The guest VLAN cannot be configured as unauthorized VLAN.

Example

The following example enables unauthorized devices access to VLAN 5.

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

dot1x authentication

To enable authentication methods on a port, use the **dot1x authentication** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x authentication [**802.1x**] [**mac**] [**web**]

no dot1x authentication

Parameters

- **802.1x**—Enables authentication based on 802.1X (802.1X-based authentication).
- **mac**—Enables authentication based on the station's MAC address (MAC-Based authentication).
- **web**—Enables WEB-Based authentication.

Default Configuration

802.1X-Based authentication is enabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Static MAC addresses cannot be authorized by the MAC-based method.

It is not recommended to change a dynamic MAC address to a static one or delete it if the MAC address was authorized by the MAC-based authentication:

1. If a dynamic MAC address authenticated by MAC-based authentication is changed to a static one, it will not be manually re-authenticated.
2. Removing a dynamic MAC address authenticated by the MAC-based authentication causes its re-authentication.

802.1x enabled on a port associated with a port channel has the following limitations:

- Only the 802.1X-based authentication is supported.
- Only the multi-host (legacy 802.1x mode) mode is supported.

Example

The following example enables authentication based on 802.1x and the station's MAC address on port gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x authentication 802.1x mac
```

dot1x credentials

To define the name of an 802.1X credential structure and enter the Dot1x credentials configuration mode, use the **dot1x credentials** command in Global Configuration mode. To remove the credential structure, use the **no** form of this command.

Syntax

dot1x credentials *name*

no dot1x credentials *name*

Parameters

- ***name***—The credential structure name up to 32 characters.

Default Configuration

A credentials structure is not specified

Command Mode

Global Configuration mode

User Guidelines

Use the **dot1x credentials** command to start configuration of credential structure. The credential structure contains the parameters of supplicant (client) and it is used during the 802.1X supplicant enabling on interface.

The credential configuration takes a place only after exit from the credential context.

Changing configuration of used credential causes supplicant logoff and logon.

The switch supports up to 24 credentials.

Use the **no dot1x credentials** command, to delete a credential. A used credential cannot be deleted.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password agrcx5642
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connected to site-A
```

dot1x eap-max-retrans

To set the EAP maximum number retransmissions, use the **dot1x eap-max-retrans** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x eap-max-retrans *count*

no dot1x eap-max-retrans

Parameters

- ***count***—Specifies the maximum number of times that the EAP Server (EAP Authenticator) retransmits an EAP request when no response from a EAP client (EAP Peer) was received. (Range: 1–10).

Default Configuration

The default maximum number of attempts is 2.

Command Mode

Interface (Ethernet, OOB) Configuration 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 parameter is used by the 802.1x Supplicant.

Example

The following example sets the EAP maximum number retransmissions to 6:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x eap-max-retrans 6
```

dot1x guest-vlan

To define a guest VLAN, use the **dot1x guest-vlan** mode command in Interface (VLAN) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Default Configuration

No VLAN is defined as a guest VLAN.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

A device can have only one global guest VLAN.

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

An unauthorized VLAN cannot be configured as guest VLAN.

Example

The following example defines VLAN 2 as a guest VLAN.

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

dot1x guest-vlan enable

To enable unauthorized users on the access interface to the guest VLAN, use the **dot1x guest-vlan enable** command in Interface Configuration mode. To disable access, use the **no** form of this command.

Syntax

dot1x guest-vlan enable

no dot1x guest-vlan enable

Default Configuration

The default configuration is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The guest VLAN and the WEB-Based authentication cannot be configured on a port at the same time.

This command cannot be configured if the monitoring VLAN is enabled on the interface.

If the port does not belong to the guest VLAN it is added to the guest VLAN as an egress untagged port.

If the authentication mode is single-host or multi-host, the value of PVID is set to the guest VLAN_ID.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs from unauthorized hosts are mapped to the guest VLAN.

If 802.1X is disabled, the port static configuration is reset.

Example

The following example enables unauthorized users on gi1/0/1 to access the guest VLAN.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x guest-vlan enable
```

dot1x guest-vlan timeout

To set the time delay between enabling 802.1X (or port up) and adding a port to the guest VLAN, use the **dot1x guest-vlan timeout** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

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 a 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
```

dot1x host-mode

To allow a single host (client) or multiple hosts on an IEEE 802.1X-authorized port, use the **dot1x host-mode** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

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 (Ethernet) Configuration mode

User Guidelines

Single-Host Mode

The single-host mode manages the authentication status of the port: the port is authorized if there is an authorized host. In this mode, only a single host can be authorized on the port.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static vlan membership configured at the port. Traffic from other hosts is dropped.

A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS-assigned VLAN or the unauthenticated VLANs.

The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.

Multi-Host Mode

The multi-host mode manages the authentication status of the port: the port is authorized after at least one host is authorized.

When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless the VLAN tag is the guest VLAN or the unauthenticated VLANs. If guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged based on the static vlan membership configured at the port.

A user can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. In this case, tagged traffic is dropped unless the VLAN tag is the RADIUS assigned VLAN or the unauthenticated VLANs.

The switch removes from FDB all MAC addresses learned on a port when its authentication status is changed from authorized to unauthorized.

Multi-Sessions Mode

Unlike the single-host and multi-host modes (port-based modes) the multi-sessions mode manages the authentication status for each host connected to the port (session-based mode). If the multi-sessions mode is configured on a port the port does have any authentication status. Any number of hosts can be authorized on the port. The command can limit the maximum number of authorized hosts allowed on the port.

Each authorized client requires a TCAM rule. If there is no available space in the TCAM, the authentication is rejected.

When using the **dot1x host-mode** command to change the port mode to **single-host** or **multi-host** when authentication is enabled, the port state is set to unauthorized.

If the **dot1x host-mode** command changes the port mode to **multi-session** when authentication is enabled, the state of all attached hosts is set to unauthorized.

To change the port mode to single-host or multi-host, set the port (**dot1x port-control**) to force-unauthorized, change the port mode to single-host or multi-host, and set the port to authorization auto.

multi-sessions mode cannot be configured on the same interface together with Policy Based VLANs configured by the following commands:

- switchport general map protocol-group vlans
- switchport general map macs-group vlans

Tagged traffic belonging to the unauthenticated VLANs is always bridged regardless if a host is authorized or not.

When the guest VLAN is enabled, untagged and tagged traffic from unauthorized hosts not belonging to the unauthenticated VLANs is bridged via the guest VLAN.

Traffic from an authorized hosts is bridged in accordance with the port static configuration. A user can specify that untagged and tagged traffic from the authorized host not belonging to the unauthenticated VLANs will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process.

The switch does not remove from FDB the host MAC address learned on the port when its authentication status is changed from authorized to unauthorized. The MAC address will be removed after the aging timeout expires.

802.1x enabled on a port associated with a port channel has the following limitations:

- Only the 802.1X-based authentication is supported.
- Only the multi-host (legacy 802.1x mode) mode is supported.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x host-mode multi-host
```

dot1x mac-auth

To specify a type (EAP or Radius), and MAC based username format, that MAC-Based authentication will use, use the **dot1x mac-auth** command in Global Configuration mode. To reset the default configuration, use the **no** form of the command.

Syntax

dot1x mac-auth {**eap** | **radius**} [**username groupsize** {**1**|**2**|**4**|**12**} **separator** {**-** | **:** |**.**} [**lowercase** | **uppercase**]]

no dot1x mac-auth

Parameters

- **eap**—Specifies that the EAP MD5-Challenge authentication is used.
- **radius**—Specifies that only Radius (without EAP) authentication with the Service-Type attribute equals to Call-Check(10) is used.
- **username**—Specifies the format of the username. If the keyword is not configured the format without separator with the lower case is applied.

username groupsize 12 separator - lowercase

- **groupsize**—Specifies the numbers of ASCII characters between delimiters.
- **separator**—Specifies the delimiter.
- **lowercase**—Specifies that the username is coded in the lower case. The argument is applied if the case argument is not configured.
- **uppercase**—Specifies that the username is coded in the upper case.

Default Configuration

EAP MD5-Challenge Authentication

Command Mode

Global Configuration mode

User Guidelines

The switch supports the following two types of MAC-Based authentication with the host MAC address as user name and password :

- EAP MD5-Challenge authentication.
- Pure Radius authentication with the Service-Type attribute equals to Call-Check(10) and with username and password in the ASCII format.

Use the **eap** keyword, to specify the EAP MD5-Challenge authentication type.

Use the **radius** keyword, to specify the pure Radius authentication type. The pure Radius authentication uses the following Radius attributes:

- User-Name: Host MAC address
- Password
- Service-Type: Call-Check(10)
- Frame-MTU
- Called-Station-Id: MAC address of the switch
- Calling-Station-Id: MAC address of the host
- Message-Authentication
- NAS-Port-Type: Ethernet(15)
- NAS-Port: ifIndex of the port where the host is connected to
- NAS-Port-Id: full CLI name of the port where the host is connected to (for example: GigabitEthernet2/0/2)
- NAS-IP-Address: IP address of the switch

Use the **username** keyword, to specify the format of the Username attributes. The following table gives examples of the Username coding for MAC address 08002b8619de:

Table 3: Examples of Username coding

Size	Separator	Username
1	-	0-8-0-0-2-b-8-6-1-9-d-e
2	:	08:00:2b:86:19:de
4	.	0800.2b86.19de
12	N/A	08002b8619de

Changing of the username format or the authentication type (EAP or Radius) causes reauthentication.

Example 1. The following example specifies that MAC-Based authentication will use the pure Radius authentication and specifies the attributes to use in username based on the station's MAC address:

switchxxxxxx(config)# dot1x mac-auth radius username groupsize 2 separator : uppercase

Example 2. The following example specifies that MAC-Based authentication will use the EAP MD5-Challenge authentication. The username format will be set to format without separator ,with lower case:

```
switchxxxxxx(config)# dot1x mac-auth eap
```

dot1x mac-auth password

To specify a global password for MAC-Based authentication, use the **dot1x mac-auth password** command in Global Configuration mode. To remove the password, use the **no** form of this command.

Syntax

encrypted dot1x mac-auth password *encrypted-password*

dot1x mac-auth password *password*

no dot1x mac-auth password

Parameters

- ***encrypted-password***—The password in encrypted format.
- ***password***—The password up to 32 characters.

Default Configuration

Username.

Command Mode

Global Configuration mode

User Guidelines

Use the command, to specify a password that will be used for MAC-Based authentication instead of the host MAC address.

Changing of the password or its format causes reauthentication.

Example

The following example configures a global password for MAC-Based authentication:

```
switchxxxxxx(config)# dot1x mac-auth password 87b$#9hv5*
```

dot1x max-hosts

To configure the maximum number of authorized hosts allowed on the interface, use the **dot1x max-hosts** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-hosts *count*

no dot1x max-hosts

Parameters

- ***count***—Specifies the maximum number of authorized hosts allowed on the interface. May be any 32 bits positive number.

Default Configuration

No limitation.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

By default, the number of authorized hosts allowed on an interface is not limited. To limit the number of authorized hosts allowed on an interface, use the **dot1x max-hosts** command.

This command is relevant only for multi-session mode.

Example

The following example limits the maximum number of authorized hosts on Ethernet port gi1/0/1 to 6:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-hosts 6
```

dot1x max-login-attempts

To set the maximum number of allowed login attempts, use the **dot1x max-login-attempts** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-login-attempts *count*

no dot1x max-login-attempts

Parameters

- ***count***—Specifies the maximum number of allowed login attempts. A value of 0 means an infinite numbers of attempts. The valid range is 3-10.

Default Configuration

Unlimited.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

By default, the switch does not limit the number of failed login attempts. To specify the number of allowed fail login attempts, use this command.

The command is applied only to the Web-based authentication.

Example

The following example sets maximum number of allowed login attempts to 5:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x max-login-attempts 5
```

dot1x max-req

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 **dot1x max-req** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x max-req *count*

no dot1x max-req

Parameters

- ***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 (Ethernet, OOB) Configuration 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 gi1/0/1
switchxxxxxx(config-if)# dot1x max-req 6
```

dot1x page customization

To enter Web-Based Page Customization Configuration mode, use the **dot1x page customization** command in Global Configuration mode.

Syntax

dot1x page customization

Default Configuration

No user customization.

Command Mode

Global Configuration mode

User Guidelines

The command should not be entered or edited manually (unless when using copy-paste). It is a part of the configuration file produced by the switch.

A user must customize the web-based authentication pages by using the browser Interface.

Example

The following example shows part of a web-based page customization configuration:

```
switchxxxxxx(config)# dot1x page customization
switchxxxxxx(config-web-page)# data 1feabcde
switchxxxxxx(config-web-page)# data 17645874
switchxxxxxx(config-web-page)# exit
```

dot1x port-control

To enable manual control of the port authorization state, use the **dot1x port-control** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x port-control {auto | **force-authorized** | **force-unauthorized**} [**time-range** *time-range-name*]

no dot1x port-control

Parameters

- **auto**—Enables 802.1X authentication on the port and causes it to transition to the authorized or unauthorized state, based on the 802.1X authentication exchange between the device and the client.
- **force-authorized**—Disables 802.1X authentication on the interface and causes the port to transition to the authorized state without any authentication exchange required. The port sends and receives 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 (Ethernet, OOB) Configuration mode

User Guidelines

802.1X authentication cannot be enabled on an interface if port security feature is already enabled on the same interface.

The switch removes all MAC addresses learned on a port when its authorization control is changed from **force-authorized** to another.



Note It is recommended to disable spanning tree or to enable spanning-tree PortFast mode on 802.1X edge 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 gi1/0/1 to auto mode.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x port-control auto
```

dot1x radius-attributes vlan

To enable RADIUS-based VLAN assignment, use the **dot1x radius-attributes vlan** command in Interface Configuration mode. To disable RADIUS-based VLAN assignment, use the **no** form of this command.

Syntax

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

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.
- **static**—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.

Default Configuration

reject

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

If RADIUS provides invalid VLAN information, the authentication is rejected.

If a RADIUS server assigns a client with a non-existing VLAN, the switch creates the VLAN. The VLAN is removed when it is no longer being used.

If RADIUS provides valid VLAN information and the port does not belong to the VLAN received from RADIUS, it is added to the VLAN as an egress untagged port. When the last authorized client assigned to the VLAN becomes unauthorized or 802.1x is disabled on the port, the port is excluded from the VLAN.

If the authentication mode is single-host or multi-host, the value of PVID is set to the VLAN_ID.

If an authorized port in the single-host or multi-host mode changes its status to unauthorized, the port static configuration is reset.

If the authentication mode is multi-sessions mode, the PVID is not changed and all untagged traffic and tagged traffic not belonging to the unauthenticated VLANs are mapped to the VLAN using TCAM.

If the last authorized host assigned to a VLAN received from RADIUS connected to a port in the multi-sessions mode changes its status to unauthorized, the port is removed from the VLAN if it is not in the static configuration.

See the User Guidelines of the **dot1x host-mode** command for more information.

If 802.1X is disabled the port static configuration is reset.

If the **reject** keyword is configured and the RADIUS server authorizes the host but the RADIUS accept message does not assign a VLAN to the supplicant, authentication is rejected.

If the **static** keyword is configured and the RADIUS server authorizes the host then even though the RADIUS accept message does not assign a VLAN to the supplicant, authentication is accepted and the traffic from the host is bridged in accordance with port static configuration.

If this command is used when there are authorized ports/hosts, it takes effect at subsequent authentications. To manually re-authenticate, use the **dot1x re-authenticate** command.

Example 1. This 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 gi1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes vlan
switchxxxxxx(config-if)# exit
```

Example 2. This 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 the static VLAN configurations is used.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x radius-attributes static
switchxxxxxx(config-if)# exit
```

dot1x re-authenticate

To initiate manually re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port, use the **dot1x re-authenticate** command in Privileged EXEC mode.

Syntax

dot1x re-authenticate [*interface-id*]

Parameters

- ***interface-id***—Specifies an Ethernet port or OOB port.

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 gi1/0/1:

```
switchxxxxxx# dot1x re-authenticate gi1/0/1
```

dot1x reauthentication

To enable periodic re-authentication of the client, use the **dot1x reauthentication** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x reauthentication

no dot1x reauthentication

Default Configuration

Periodic re-authentication is disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x reauthentication
```

dot1x supplicant

To enable the dot1x supplicant role for a given interface, use the **dot1x supplicant** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x supplicant *name*

no dot1x supplicant

Parameters

- ***name***—The name of the credential structure applied on the interface.

Default Configuration

The supplicant role is disabled.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

Use the **dot1x supplicant** command to enable the dot1x supplicant on a given interface. When the supplicant is enabled on an interface the interface becomes an unauthorized. When the 802.1X authentication successes the interface state is changed to authorized.

If the *name* argument specifies an undefined or not fully defined (password or username is not configured) 802.1X credential structure, the command is rejected.

Authenticator and Supplicant cannot be enabled together on the same interface.

The command cannot be configured a few times on the same port. To replace the configured credential, use the **no** form of the command before configuration a new credential.

Unlike unauthorized authenticator interface an unauthorized supplicant interface does not limit any traffic passed through.

The following events start the 802.1X supplicant authentication on a port:

- The **dot1x supplicant** command enables the supplicant on the port in the UP status.
- The status of the port is changed to UP and the supplicant is enabled on the port.
- The EAP Identifier Request message is received on the port and the supplicant is enabled on the port.

Example

The following example configures an 802.1X supplicant on port gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x supplicant upstream-port
```

dot1x supplicant traps authentication failure

To enable sending traps when an 802.1X supplicant authentication fails, use the **dot1x supplicant traps authentication failure** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x supplicant traps authentication failure

no dot1x supplicant traps authentication failure

Default Configuration

Traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when an 802.1X supplicant authentication failed:

```
switchxxxxxx(config)# dot1x supplicant traps authentication failure
```

dot1x supplicant traps authentication success

To enable sending traps when an 802.1X supplicant authentication is succeeded, use the **dot1x supplicant traps authentication success** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x supplicant traps authentication success

no dot1x supplicant traps authentication success

Default Configuration

Traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when an 802.1X supplicant authentication is succeeded:

```
switchxxxxxx(config)# dot1x supplicant traps authentication success
```

dot1x system-auth-control

To enable 802.1X globally, use the **dot1x system-auth-control** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x system-auth-control

no dot1x system-auth-control

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

The following example enables 802.1X globally.

```
switchxxxxxx(config)# dot1x system-auth-control
```

dot1x timeout eap-timeout

To set the EAP timeout, use the **dot1x timeout eap-timeout** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout eap-timeout *seconds*

no dot1x timeout eap-timeout

Parameters

- ***seconds***—Specifies the time interval in seconds during which the EAP Server (EAP Authenticator) waits for a response from the EAP client (EAP Peer) before the request retransmission. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 30 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration 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 parameter is used by the 802.1x Supplicant.

Example

The following example sets the EAP timeout to 45 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout eap-timeout 45
```

dot1x timeout quiet-period

To set the time interval that the device remains in a quiet state following a failed authentication exchange, use the **dot1x timeout quiet-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

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 a client. (Range: 10–65535 seconds).

Default Configuration

The default quiet period is 60 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration 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 and MAC-based authentication, the number of failed logins is 1.

For WEB-based authentication, the quiet period is applied after a number of failed attempts.

For 802.1x-based and MAC-based authentication methods, the quiet 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 gi1/0/1
switchxxxxxx(config-if)# dot1x timeout quiet-period 120
```

dot1x timeout reauth-period

To set the number of seconds between re-authentication attempts, use the **dot1x timeout reauth-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, OOB) Configuration mode

User Guidelines

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

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout reauth-period 5000
```

dot1x timeout server-timeout

To set the time interval during which the device waits for a response from the authentication server, use the **dot1x timeout server-timeout** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, OOB) Configuration mode

User Guidelines

The actual timeout period can be determined by comparing the value specified by this 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 transmit 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 gi1/0/1
switchxxxxxx(config-if)# dot1x timeout server-timeout 3600
```

dot1x timeout silence-period

To set the authentication silence time, use the **dot1x timeout silence-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x timeout silence-period *seconds*

no dot1x timeout silence-period

Parameters

- ***seconds***—Specifies the silence interval in seconds. The valid range is 60 - 65535.

Default Configuration

The silence period is not limited.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The silence time is the number of seconds that if an authorized client does not send traffic during this period, the client is changed to unauthorized.

If an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.

The command is only applied to WEB-based authentication.

Example

The following example sets the authentication silence time to 100 seconds:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout silence-period 100
```

dot1x timeout supp-timeout

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 **dot1x timeout supp-timeout** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, OOB) Configuration 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 gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supp-timeout 3600
```

dot1x timeout supplicant-held-period

To set the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the Radius server, use the **dot1x timeout supplicant-held-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command

Syntax

dot1x timeout supplicant-held-period *seconds*

no dot1x timeout supplicant-held-period

Parameters

- ***seconds***—Specifies the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the Radius server. (Range: 1–65535 seconds).

Default Configuration

The default timeout period is 60 seconds.

Command Mode

Interface (Ethernet, OOB) Configuration mode

User Guidelines

The default value of this command should be changed only to adjust to unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Example

The following example sets the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the Radius server to 70 seconds.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x timeout supplicant-held-period 70
```

dot1x timeout tx-period

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 **dot1x timeout tx-period** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, OOB) Configuration 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 gi1/0/1:
switchxxxxxx(config-if)# dot1x timeout tx-period 60
```

dot1x traps authentication failure

To enable sending traps when an 802.1X authentication method failed, use the **dot1x traps authentication failure** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x traps authentication failure {[**802.1x**] [**mac**] [**web**]}

no dot1x traps authentication failure

Parameters

- **802.1x**—Enables traps for 802.1X-based authentication.
- **mac**—Enables traps for MAC-based authentication.
- **web**—Enables traps for WEB-based authentication.

Default Configuration

All traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

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)# dot1x traps authentication failure 802.1x
```

dot1x traps authentication quiet

To enable sending traps when a host state is set to the quiet state after failing the maximum sequential attempts of login, use the **dot1x traps authentication quiet** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

Syntax

dot1x traps authentication quiet

no dot1x traps authentication quiet

Default Configuration

Quiet traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

The traps are sent after the client is set to the quiet state after the maximum sequential attempts of login.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a host is set in the quiet state:

```
switchxxxxxx(config)# dot1x traps authentication quiet
```

dot1x traps authentication success

To enable sending traps when a host is successfully authorized by an 802.1X authentication method, use the **dot1x traps authentication success** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

Syntax

dot1x traps authentication success {[**802.1x**] [**mac**] [**web**]}

no dot1x traps authentication success

Parameters

- **802.1x**—Enables traps for 802.1X-based authentication.
- **mac**—Enables traps for MAC-based authentication.
- **web**—Enables traps for WEB-based authentication.

Default Configuration

Success traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

Any combination of the keywords are allowed. At least one keyword must be configured.

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a MAC address is successfully authorized by the 802.1X MAC-authentication access control.

```
switchxxxxxx(config)# dot1x traps authentication success mac
```

dot1x unlock client

To unlock a locked (in the quiet period) client, use the **dot1x unlock client** command in Privileged EXEC mode.

Syntax

dot1x unlock client *interface-id mac-address*

Parameters

- ***interface-id***—Interface ID where the client is connected to.
- ***mac-address***—Client MAC address.

Default Configuration

The client is locked until the silence interval is over.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to unlock a client that was locked after the maximum allowed authentication failed attempts and to end the quiet period. If the client is not in the quiet period, the command has no affect.

Example

```
switchxxxxxx# dot1x unlock client gi1/0/1 00:01:12:af:00:56
```

dot1x violation-mode

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 **dot1x violation-mode** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

dot1x violation-mode {restrict | **protect** | **shutdown**} [**traps** *seconds*]

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 addresses are not learned.
- **protect**—Discard frames with source addresses that are not the supplicant address.
- **shutdown**—Discard frames with source addresses that are not the supplicant address and shutdown the port.
- **trap** *seconds* - Send SNMP traps, and specifies the minimum time between consecutive traps. If seconds = 0 traps are disabled. If the parameter is not specified, it defaults to 1 second for the restrict mode and 0 for the other modes.

Default Configuration

Protect

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The command is relevant only for single-host mode.

For BPDU messages whose MAC addresses are not the supplicant MAC address are not discarded in Protect mode.

BPDU message whose MAC addresses are not the supplicant MAC address cause a shutdown in Shutdown mode.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# dot1x violation-mode protect
```

password

To specify a password for an 802.1X credential structure, use the **password** command in Dot1x credentials configuration mode. To remove the password, use the **no** form of this command.

Syntax

encrypted password *encrypted-password*

password *password*

no password

Parameters

- ***encrypted-password***—The password in encrypted format.
- ***password***—The password up to 64 characters.

Default Configuration

A password is not specified.

Command Mode

Dot1x credentials configuration mode

User Guidelines

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure must contain a username and password and might contain a description.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 87b$#9hv5*
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connect to site-A.
```

show dot1x

To display the 802.1X interfaces or specified interface status, use the **show dot1x** command in Privileged EXEC mode.

Syntax

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

Parameters

- ***interface-id***—Specifies an Ethernet port or OOB 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

Example

The following example displays authentication information for all interfaces on which 802.1x is enabled:

```
switchxxxxxx# show dot1x
Authentication is enabled
Authenticator Global Configuration:
Authenticating Servers: Radius, None
MAC-Based Authentication:
  Type: Radius
  Username Groupsize: 2
  Username Separator: -
  Username case: Lowercase
  Password: MD5 checksum 1238af77aaca17568f12988601fcabed
Unathenticated VLANs: 100, 1000, 1021
Guest VLAN: VLAN 11, timeout 30 sec
Authentication failure traps are enabled for 802.1x+mac
Authentication success traps are enabled for 802.1x
Authentication quiet traps are enabled for 802.1x
Supplicant Global Configuration:
Supplicant Authentication failure traps are enabled
Supplicant Authentication success traps are enabled
gi1/0/1
  Authenticator is enabled
  Supplicant is disabled
```

```
  Authenticator Configuration:
  Host mode: multi-sessions
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Guest VLAN: enabled
  VLAN Radius Attribute: enabled, static
  Open access: disabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Maximum Hosts: unlimited
  Maximum Login Attempts: 3
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 9
  Authentication fails: 1
  Number of Authorized Hosts: 10
  Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gi1/0/2
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: single-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: enabled
  Open access: enabled
  Time range name: work_hours (Active now)
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 9
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 2
  Authentication fails: 0
gi1/0/3
```

```
  Authenticator is enabled
  Supplicant is disabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: auto
  Port Operational status: authorized
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
  Interfaces 802.1X-Based Parameters
    EAP Timeout: 30 sec
    EAP Max-Retrans: 2
    Tx period: 30 sec
    Supplicant timeout: 30 sec
    max-req: 2
  Authentication success: 20
  Authentication fails: 0
  Supplicant Configuration:
  retry-max: 2
  EAP time period: 15 sec
  Supplicant Held Period: 30 sec
gi1/0/4
  Authenticator is disabled
  Supplicant is enabled
  Authenticator Configuration:
  Host mode: multi-host
  Authentication methods: 802.1x+mac
  Port Adminstrated status: force-auto
  Guest VLAN: disabled
  VLAN Radius Attribute: disabled
  Time range name: work_hours (Active now)
  Open access: disabled
  Server-timeout: 30 sec
  Aplied Authenticating Server: Radius
  Applied Authentication method: 802.1x
  Session Time (HH:MM:SS): 00:25:22
  MAC Address: 00:08:78:32:98:66
  Username: Bob
  Violation:
    Mode: restrict
    Trap: enabled
    Trap Min Interval: 20 sec
    Violations were detected: 0
  Reauthentication is enabled
  Reauthentication period: 3600 sec
  Silence period: 1800 sec
  Quiet Period: 60 sec
```

```
Interfaces 802.1X-Based Parameters
  EAP Timeout: 30 sec
  EAP Max-Retrans: 2
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  max-req: 2
Authentication success: 0
Authentication fails: 0
Supplicant Configuration:
retry-max: 2
EAP time period: 15 sec
Supplicant Held Period: 30 sec
Credentials Name: Basic-User
Supplicant Operational status: authorized
```

The following describes the significant fields shown in the display:

- **Port**—The port interface-id.
- **Host mode**—The port authentication configured mode. Possible values: single-host, multi-host, multi-sessions.
  - single-host
  - multi-host
  - multi-sessions
- **Authentication methods**—Authentication methods configured on port. Possible values are combinations of the following methods:
  - 802.1x
  - mac
  - wba
- **Port Administrated status**—The port administration (configured) mode. Possible values: **force-auth**, **force-unauth**, **auto**.
- **Port Operational status**—The port operational (actual) mode. Possible values: **authorized** or **unauthorized**.
- **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).
- **Silence period**—Number of seconds that If an authorized client does not send traffic during the silence period specified by the command, the state of the client is changed to unauthorized.
- **EAP timeout**—Time interval in seconds during which the EAP Server (EAPAuthenticator) waits for a response from the EAP client (EAP Peer) before the requestretransmission
- **EAP Max Retrans**—Maximum number of times that the EAP Server (EAPAuthenticator) retransmits an EAP request when no response from a EAP client (EAPPeer) was received.

- **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.
- **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 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.

show dot1x credentials

To display 802.1X credentials, use the **show dot1x credentials** mode command in Privileged EXEC mode.

Syntax

show dot1x credentials

Command Mode

Privileged EXEC mode

Examples

The following example displays dot1x credentials:

```
switchxxxxxx# show dot1x credentials
downstream-interface
 description: should be used for downstream ports
 username: downstream
 password's MD5: 1238af77aaca17568f12988601fcabed
upstream-interface
 description: should be used for connection to ISP
 username: up2isp
 password's MD5: 1238bbff75431230965394466ac76549
```

show dot1x locked clients

To display all clients who are locked and in the quiet period, use the **show dot1x locked clients** command in Privileged EXEC mode.

Syntax

show dot1x locked clients

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show dot1x locked clients** command to display all locked (in the quiet period) clients.

Example

The following example displays locked clients:

```
switchxxxxxx# show dot1x locked clients
```

Port	MAC Address	Remaining Time
-------	-------------	-------------
gi1/0/1	0008.3b79.8787	20
gi1/0/1	0008.3b89.3128	40
gi1/0/2	0008.3b89.3129	10

show dot1x sessions interface

To display active 802.1X sessions for the specified interface, use the show dot1x sessions interface command in Privileged EXEC mode.

Syntax

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

Parameters

- **interface** *interface-id* —Specifies an Ethernet port.
- **detailed** (optional) — displays detailed information for each session on the interface.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to display the list of 802.1x sessions on the interface. A session can be authorized or authenticated but not authorized.

If the detailed keyword is not specified then the command output will provide the following information for each session: the interface for which the command output was requested, the MAC address of the supplicant, the method in which the supplicant was authenticated (MAC, dot1x or WBA), the session status - Auth (authenticated) or Unauth (authenticated but not authorized) and the Session ID.

If the detailed keyword is specified then the command output will provide, in addition, the following information for each session: the supplicant IPv4 address (if known), the supplicant username, the reason for Unauthorized stated (if relevant), the interface Oper host mode, the session re-authentication timeout value and the seconds remaining until tineout, timeout action, the session up time, the Common Session ID (audit session ID) and the accounting session ID. In addition the output may detail the Server Policies that are applied to the session.

This includes downloadable ACLs redirect ACL and redirect URL.

Example

Example 1. The following example displays 802.1X sessions on interface gi1 without using the detailed keyword.

```
switchxxxxxx# show dot1x session interface gi1
Interface Mac Address Method Status Session ID
---------- ----------------- -------- -------- ------------------------
gi1 68:05:ca:21:28:e6 MAC Auth 8787020A05000003000278A8
```

Example 2. The following example displays 802.1X sessions on interface gi1 including the detailed keyword.

```
switchxxxxxx# show dot1x session interface gi1 detailed
Interface: gi1
MAC Address: 68:05:ca:21:28:e6
IPv4 Address: 10.2.135.69
User-Name: guest1
Status: Authorized
Oper host mode: multi-session
Session timeout: 300 sec, Remaining: 92 sec
Timeout action: Reauthenticate
Session Uptime: 13708 sec
Common Session ID: 8787020A05000003000278A8
Acct Session ID: 0x05000003
Server Policies:
URL Redirect ACL: redirect_ACL
URL Redirect:
https://ise-svr.company.com:8443/portal/gateway?sessionId=8787020A05000003000278
A8&portal=f09aaac2-f101-45ed-832f-fda201ab7639&action=cwa&token=2289745240da1822
bf2c7a8af4a08452
ACS ACL: xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
Method status list:
Method State
MAC Authentication success
```

show dot1x statistics

To display 802.1X statistics for the specified port, use the **show dot1x statistics** command in Privileged EXEC mode.

Syntax

show dot1x statistics interface *interface-id*

Parameters

- ***interface-id***—Specifies an Ethernet port or OOB port.

Command Mode

Privileged EXEC mode

Example

The following example displays 802.1X statistics for gi1/0/1.

```
switchxxxxxx# show dot1x statistics interface gi1/0/1
EapolEapFramesRx: 10
EapolStartFramesRx: 0
EapolLogoffFramesRx: 1
EapolAnnouncementFramesRx: 0
EapolAnnouncementReqFramesRx: 0
EapolInvalidFramesRx: 0
EapolEapLengthErrorFramesRx: 0
EapolMkNoCknFramesRx: 0
EapolMkInvalidFramesRx: 0
EapolLastRxFrameVersion: 3
EapolLastRxFrameSource: 00:08:78:32:98:78
EapolSuppEapFramesTx: 0
EapolStartFramesTx: 1
EapolLogoffFramesTx: 0
EapolAnnouncementFramesTx: 0
EapolAnnouncementReqFramesTx: 0
EapolAuthEapFramesTx: 9
EapolMkaFramesTx: 0
```

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

Field	Description
EapolInvalidFramesRx	The number of invalid EAPOL frames of any type that have been received by this PAE.
EapolEapLengthErrorFramesRx	The number of EAPOL frames that the Packet Body Length does not match a Packet Body that is contained within the octets of the received EAPOL MPDU in this PAE.
EapolAnnouncementFramesRx	The number of EAPOL-Announcement frames that have been received by this PAE.
EapolAnnouncementReqFramesRx	The number of EAPOL-Announcement-Req frames that have been received by this PAE.
EapolStartFramesRx	The number of EAPOL-Start frames that have been received by this PAE.
EapolEapFramesRx	The number of EAPOL-EAP frames that have been received by this PAE.
EapolLogoffFramesRx	The number of EAPOL-Logoff frames that have been received by this PAE.
EapolMkNoCknFramesRx	The number of MKPDUs received with MKA not enabled or CKN not recognized in this PAE.
EapolMkInvalidFramesRx	The number of MKPDUs failing in message authentication on receipt process in this PAE.

Field	Description
EapolLastRxFrameVersion	The version of last received EAPOL frame by this PAE.
EapolLastRxFrameSource	The source MAC address of last received EAPOL frame by this PAE.
EapolSuppEapFramesTx	The number of EAPOL-EAP frames that have been transmitted by the supplicant of this PAE.
EapolLogoffFramesTx	The number of EAPOL-Logoff frames that have been transmitted by this PAE.
EapolAnnouncementFramesTx	The number of EAPOL-Announcement frames that have been transmitted by this PAE.
EapolAnnouncementReqFramesTx	The number of EAPOL-Announcement-Req frames that have been transmitted by this PAE.
EapolStartFramesTx	The number of EAPOL-Start frames that have been received by this PAE.
EapolAuthEapFramesTx	The number of EAPOL-EAP frames that have been transmitted by the authenticator of this PAE.
EapolMkaFramesTx	The number of EAPOL-MKA frames with no CKN information that have been transmitted by this PAE.

show dot1x users

To display active 802.1X authorized users for the device, use the **show dot1x users** command in Privileged EXEC mode.

Syntax

show dot1x users [username *username*]

Parameters

- **username** username—Specifies the supplicant username (Length: 1–160 characters).

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example 1. The following commands displays all 802.1x users:

```
show dot1x users
```

Port	Username	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020
gi1/0/2	00083b798787	0008.3b79.8787	MAC	Remote	00:11:12	
gi1/0/2	John	0008.3baa.0022	WBA	Remote	00:27:16	

Example 2. The following example displays 802.1X user with supplicant username Bob:

```
switchxxxxxx# show dot1x users username Bob
```

Port	Username	MAC Address	Auth Method	Auth Server	Session Time	VLAN
gi1/0/1	Bob	0008.3b71.1111	802.1x	Remote	09:01:00	1020

username (dot1x credentials)

To specify a username for an 802.1X credential structure, use the **username** command in Dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

Syntax

username *username*

no username

Parameters

- ***username***—The user name up to 32 characters.

Default Configuration

A username is not specified.

Command Mode

Dot1x credentials configuration mode

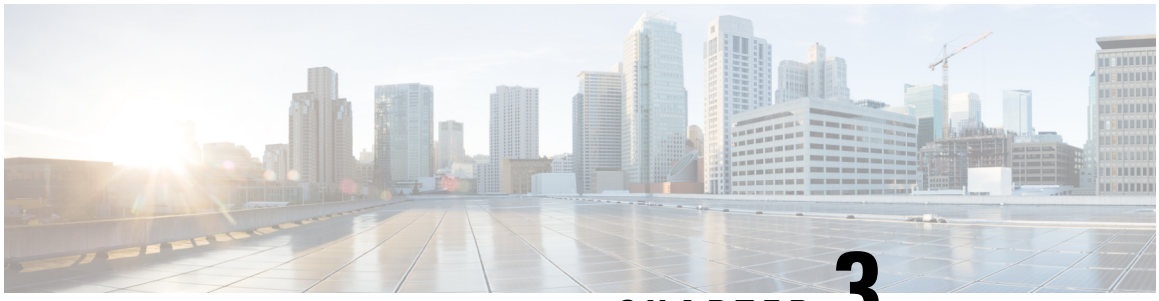
User Guidelines

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure may contain a username, password, and description.

Example

The following example configures an 802.1X credential structure:

```
switchxxxxxx(config)# dot1x credentials site-A
switchxxxxxx(config-dot1x-cred)# username inner-switch
switchxxxxxx(config-dot1x-cred)# password 87%$#bgd98^
switchxxxxxx(config-dot1x-cred)# description This credentials profile should be used to
connected to site-A
```



CHAPTER 3

ACL Commands

This chapter contains the following sections:

- ip access-list (IP extended), on page 63
- permit (IP), on page 64
- deny (IP), on page 66
- ipv6 access-list (IPv6 extended), on page 69
- permit (IPv6), on page 70
- deny (IPv6), on page 72
- mac access-list, on page 74
- permit (MAC), on page 75
- deny (MAC), on page 76
- service-acl input, on page 77
- service-acl output, on page 78
- time-range, on page 79
- absolute, on page 80
- periodic, on page 81
- show time-range, on page 82
- show access-lists, on page 83
- show ip access-lists, on page 83
- clear access-lists counters, on page 84
- show interfaces access-lists trapped packets, on page 85
- ip access-list (IP standard), on page 85
- ipv6 access-list (IP standard), on page 87

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), on page 64 and deny (IP), on page 66 commands. The service-acl input, on page 77 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-nam*e

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)#
```

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*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

permit tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]**

permit udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard}* [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

no permit *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]**

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*] [**time-range** *time-range-name*] [**log-input]**

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*] [**time-range** *time-range-name*] [**log-input]**

Parameters

- ***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.
- ***priority*** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- **dscp** *number*—Specifies the DSCP value.
- **precedence** *number*—Specifies the IP precedence value.
- ***icmp-type***—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- ***icmp-code***—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- ***igmp-type***—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- ***destination-port***—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp

(25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177).(Range: 0–65535).

- ***source-port***—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all** *list-of-flags*—List of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **log-input**—Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an 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

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.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
```

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*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port**|**log-input**]

deny *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]][**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*][**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny tcp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*}{**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**match-all** *list-of-flags*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

deny udp {**any** | *source source-wildcard*} {**any**|*source-port/port-range*} {**any** | *destination destination-wildcard*} {**any**|*destination-port/port-range*} [**ace-priority** *priority*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input** *]*

no deny *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny *icmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*]] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

no deny *igmp* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*}[*igmp-type*] [**dscp** *number* | **precedence** *number*][**time-range** *time-range-name*] [**disable-port** |**log-input** *]*

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*] [**time-range** *time-range-name*] [**disable-port** |**log-input**]

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*][**time-range** *time-range-name*] [**disable-port** |**log-input**]

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.
- ***priority*** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- **dscp** *number*—Specifies the DSCP value.

- **precedence** *number*—Specifies the IP precedence value.
- ***icmp-type***—Specifies an ICMP message type for filtering ICMP packets. Enter a number or one of the following values: echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris. (Range: 0–255)
- ***icmp-code***—Specifies an ICMP message code for filtering ICMP packets. (Range: 0–255)
- ***igmp-type***—IGMP packets can be filtered by IGMP message type. Enter a number or one of the following values: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3. (Range: 0–255)
- ***destination-port***—Specifies the UDP/TCP destination port. You can enter range of ports by using hyphen. E.g. 20 - 21. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp 161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- ***source-port***—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- **match-all** *list-of-flags*—List of TCP flags that should occur. If a flag should be set it is prefixed by “+”.If a flag should be unset it is prefixed by “-”. Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- **time-range-name**—Name of the time range that applies to this permit statement. (Range: 1–32)
- **disable-port**—The Ethernet interface is disabled if the condition is matched.
- **log-input**—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an 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.

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Example

```
switchxxxxxx(config)# ip access-list extended server
switchxxxxxx(config-ip-al)# deny ip 176.212.0.0 00.255.255 any
```

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.

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

```
switchxxxxxx(config)#  ipv6 access-list acl1
switchxxxxxx(config-ip-al)#  permit tcp 2001:0DB8:0300:0201::/64 any any 80
```

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*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input**] [**flow-label** *flow-label-value*]

permit icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

permit tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any** | *destination-port*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

permit udp {any | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any** | *destination-port*} [**ace-priority** *priority*][**dscp** *number* | precedence *number*][**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit *protocol* {**any** |{*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/length} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit tcp {**any** | {*source-prefix*/*length*} {**any** | source-port}}{**any** | destination- prefix/length} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

no permit udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**log-input]** [**flow-label** *flow-label-value*]

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 / lenght***—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/ lenght***—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.
- ***priority*** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- ***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. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- ***source-port***—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- ***match-all list-of-flag*** —List of TCP flags that should occur. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- ***time-range-name***—Name of the time range that applies to this permit statement. (Range: 1–32)
- **log-input**—Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an 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.
- **flow-label** *flow-label-value*—Specifies the IPv6 Flow Label value. A value of these arguments must be in range 0–1048575.

Default Configuration

No IPv6 access list is defined.

Command Mode

Ipv6 Access-list Configuration mode

User Guidelines

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Flow label and port range cannot be configured together.

Flow label cannot be configured into an output ACL.

Example 1. 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
```

Example 2. This example defines an ACL with the **flow-label** keyword:

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# permit ipv6 any any flow-label 5
```

deny (IPv6)

Use the **deny** command in Ipv6 Access-list Configuration mode to set deny 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*} [**ace-priority** *priority]*[**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**ace-priority** *priority*][**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

deny udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} *[***ace-priority** *priority]*[**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny *protocol* {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny icmp {**any** | {*source-prefix*/*length*}{**any** | *destination-prefix*/*length*} {**any**|*icmp-type*} {**any**|*icmp-code*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny tcp {**any** | {*source-prefix*/*length*} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

no deny udp {**any** | {*source-prefix*/*length*}} {**any** | *source-port*}}{**any** | *destination-prefix*/*length*} {**any**| *destination-port*} [**dscp** *number* | **precedence** *number*] [**time-range** *time-range-name*] [**disable-port** |**log-input**] [**flow-label** *flow-label-value*]

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 / lenght***—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.
- ***priority*** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- ***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. For TCP enter a number or one of the following values: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data 20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). For UDP enter a number or one of the following values: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), non500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). (Range: 0–65535)
- ***source-port***—Specifies the UDP/TCP source port. Predefined port names are defined in the destination-port parameter. (Range: 0–65535)
- ***match-all list-of-flags***—List of TCP flags that should occur. If a flag should be set it is prefixed by "+".If a flag should be unset it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. The flags are concatenated to a one string. For example: +fin-ack.
- ***time-range-name***—Name of the time range that applies to this permit statement. (Range: 1–32)
- ***disable-port***—The Ethernet interface is disabled if the condition is matched.
- ***log-input***—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an 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.
- ***flow-label flow-label-value***—Specifies the IPv6 Flow Label value. A value of these arguments must be in range 0–1048575.

Default Configuration

No IPv6 access list is defined.

Command Mode

Ipv6 Access-list Configuration mode

User Guidelines

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

Flow label and port range cannot be configured together.

Flow label cannot be configured into an output ACL.

Example

```
switchxxxxxx(config)# ipv6 access-list server
switchxxxxxx(config-ipv6-al)# deny tcp 3001::2/64 any any 80
```

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.

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. If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

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
```

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} [***ace-priority** *priority][eth-type 0* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name]*

*[***log-input]**

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] [***time-range** *time-range-name]*

*[***log-input]**

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.
- ***priority*** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- ***eth-type***—The Ethernet type in hexadecimal format of the packet.
- ***vlan-id***—The VLAN ID of the packet. (Range: 1–4094)
- ***cos***—The Class of Service of the packet. (Range: 0–7)
- ***cos-wildcard***—Wildcard bits to be applied to the CoS.
- ***time-range-name***—Name of the time range that applies to this permit statement. (Range: 1–32)
- **log-input**—Specifies sending an informational SYSLOG message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an 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.

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 If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE

(in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

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
```

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} [***ace-priority** *priority][{eth-type 0}|* **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000***] [***vlan** *vlan-id] [***cos** *cos cos-wildcard] [***time-range** *time-range-name] [***disable-port** |**log-input** *]*

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] [***time-range** *time-range-name] [***disable-port** |**log-input** *]*

Parameters

- ***source***—Source MAC address of the packet.
- ***source-wildcard***—Wildcard bits to be applied to the source MAC address. Use ones in the bit position that you want to be ignored.
- ***destination***—Destination MAC address of the packet.
- ***destination-wildcard***—Wildcard bits to be applied to the destination MAC address. Use 1s in the bit position that you want to be ignored.
- ***priority*** - Specify the priority of the access control entry (ACE) in the access control list (ACL). "1" value represents the highest priority and "2147483647" number represents the lowest priority.(Range: 1-2147483647)
- ***eth-type***—The Ethernet type in hexadecimal format of the packet.
- ***vlan-id***—The VLAN ID of the packet. (Range: 1–4094).
- ***cos***—The Class of Service of the packet.(Range: 0–7).
- ***cos-wildcard***—Wildcard bits to be applied to the CoS.
- ***time-range-name***—Name of the time range that applies to this permit statement. (Range: 1–32)

- ***disable-port***—The Ethernet interface is disabled if the condition is matched.
- ***log-input***—Specifies sending an informational syslog message about the packet that matches the entry. Because forwarding/dropping is done in hardware and logging is done in software, if a large number of packets match an ACE containing a log-input keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

Default Configuration

No MAC access list is defined.

Command Mode

MAC Access-list Configuration mode

User Guidelines

A MAC ACL is defined by a unique name. IPv4 ACL, IPv6 ACL, MAC ACL or policy maps cannot have the same name

If ace-priority is omitted, the system sets the rule's priority to the current highest priority ACE (in the current ACL) + 20. The ACE-priority must be unique per ACL.If the user types already existed priority, then the command is rejected.

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
```

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. Default action for ACL is deny-any.

Command Mode

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

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.
- MAC ACLs that include a VLAN as match criteria cannot be bound to a VLAN.
- ACLs with time-based configuration on one of its ACEs cannot be bound to a VLAN.
- ACLs with the action Shutdown cannot be bound to a VLAN.
- When the user binds ACL to an interface, TCAM resources will be consumed. One TCAM rule for each MAC or IP ACE and two TCAM rules for each IPv6 ACE.The TCAM consumption is always even number, so in case of odd number of rules the consumption will be increased by 1.
- An ACL cannot be bound as input if it has been bound as output.

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 gi1/0/1
switchxxxxxx(config-if)# service-acl input server-acl default-action deny-any
```

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*] [**default-action** {**deny-any** | **permit-any**}]

no service-acl output

Parameters

- ***acl-name***—Specifies an ACL to apply to the interface. See the user guidelines. (Range: 1–32 characters).
- **deny-any**—Deny all packets (on the output of port) that do not meet the rules in this ACL.

- **permit-any**—Forward all packets (on the output of port) that do not meet the rules in this ACL.

Default

No ACL is assigned. Default action is deny-any

Command Mode

Interface Configuration mode(Ethernet, Port-Channel).

User Guidelines

The rule actions: log-input is not supported. Trying to use it will result in an error.

The deny rule action disable-port is not supported. Trying to use it 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.

An ACL cannot be bound as output if it has been bound as input.

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 gi1/0/1
switchxxxxxx(config-if)# service-acl output server
```

time-range

Use the **time-range** Global Configuration mode command to define time ranges for different 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, on page 80 and periodic, on page 81 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

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.

When a time range is defined, it can be used in the following commands:

- dot1x port-control
- power inline
- operation time
- permit (IP)
- deny (IP)
- permit (IPv6)
- deny (IPv6)
- permit (MAC)
- deny (MAC)

Example

```
switchxxxxxx(config)# time-range http-allowed
console(config-time-range)#periodic mon 12:00 to wed 12:00
```

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
```

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 *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-week**—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
```

show time-range

Use the **show time-range** User EXEC mode 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

User 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
```

show access-lists

Use the **show access-lists** Privileged EXEC mode command to display access control lists (ACLs) configured on the switch.

Syntax

show access-lists [*name*]

show access-lists *time-range-active* *[name]*

Parameters

- **name**—Specifies the name of the ACL.(Range: 1-160 characters).
- **time-range-active**—Shows only the Access Control Entries (ACEs) whose time-range is currently active (including those that are not associated with time-range).

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show access-lists
Standard IP access list 1
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any priority 20 time-range weekdays
permit 234 172.30.23.8 0.0.0.255 any priority 40 time-range weekdays
switchxxxxxx# show access-lists time-range-active
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8  0.0.0.0 any priority 40
Extended IP access list ACL2
permit 234 172.30.19.1 0.0.0.255 any priority 20  time-range weekdays
switchxxxxxx# show access-lists ACL1
Extended IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any priority 20
permit 234 172.30.8.8  0.0.0.0 any priority 40
```

show ip access-lists

Use the show ip access-lists Privileged EXEC mode command to display IP Extended access control lists (ACLs) configured on the switch or on a specific interface.

Syntax

show ip access-lists [interface *interface-id***] [brief]**

Parameters

- **interface** interface-id (optional) —displays the IP ACLs on the specified interface.

- **brief** (optional) - displays the list of IP ACLs without the rules

Command Mode

Privileged EXEC mode

User Guidelines

Use this command without the interface parameter to display all of the IP extended access lists that are configured on the device. ACLs that were created dynamically on the device will have the (per user) indication alongside the ACL name.

Use this command with the interface parameter to display only the ACLs and rules that are applied to the specified interface. With this option the rules will be displayed with the actual classification values that were configured on the interface.

Examples

Example 1- The following example displays the list of all of the IP extended access lists that are configured on the device.

```
switchxxxxxx# show ip access-lists
ip access-list extended acl1
permit ip any host 10.1.1.1 ace-priority 20
deny tcp any www any 90 ace-priority 40 disable
ip access-list extended acl2
permit ip any any ace-priority 20
ip access-list extended xACSACLx-IP-permit-any-66cee2c6 (per-user)
permit ip any any ace-priority 1
```

Example 2- The following example displays the list of all of the IP extended access lists that are configured on interface gi1.

```
switchxxxxxx# show ip access-list interface gi1
ip access-list extended xACSACLx-IP-permit-any-66cee2c6 (per-user)
permit ip host 10.2.135.69 any ace-priority 1
ip access-list extended acl2
permit ip any any ace-priority 20
```

Example 3- The following example displays only the names of the IP extended access lists that are configured on interface gi1, without the ACL rules.

```
switchxxxxxx# show ip access-list interface gi1 brief
ip access-list extended xACSACLx-IP-permit-any-66cee2c6 (per-user)
ip access-list extended acl2
```

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 gi1/0/1
```

show interfaces access-lists trapped packets

Use the **show interfaces access-lists trapped packets** Privileged EXEC mode command to display Access List (ACLs) trapped packets.

Syntax

show interfaces access-lists trapped packets *[interface-id | port-channel-number | VLAN]*

Parameters

- **interface-id**—Specifies an interface ID, the interface ID is an Ethernet port port-channel.
- **port-channel**—Specifies a port-channel.
- **VLAN**—Specifies a VLAN

Command Mode

Privileged EXEC mode

User Guidelines

This command shows whether packets were trapped from ACE hits with logging enable on an interface.

Example 1:

```
switchxxxxxx# show interfaces access-lists trapped packets
Ports/LAGs: gi1/0/1-gi1/0/3, ch1-ch3, ch4
VLANs: VLAN1, VLAN12-VLAN15
Packets were trapped globally due to lack of resources
```

Example 2:

```
switchxxxxxx# show interfaces access-lists trapped packets gi1/0/1
Packets were trapped on interface gi1/0/1
```

ip access-list (IP standard)

Use the **ip access-list** Global Configuration mode command to define an IP standard list. The **no** format of the command removes the list.

Syntax

ip access-list *access-list-name* {**deny**|**permit**} {*src-addr*[/*src-len*] | **any**}

no ip access-list *access-list-name*

Parameters

- **access-list-name**—The name of the Standard IP access list. The name may contain maximum 32 characters.
- **deny/permit**—Denies/permits access if the conditions are matched.

  src-addr[/*src-len*] | **any**— IP prefix defined as an IP address and length or **any**. The **any** value matches all IP addresses. If *src-len* is not defined, a value of 32 is applied. A value of *src-len* must be in the interval 1-32.

Default Configuration

No access list is defined.

Command Mode

Global Configuration mode

User Guidelines

Use the **ip access-list** command to configure IP address filtering. Access lists are configured with **permit** or **deny** keywords to either permit or deny an IP address based on a matching condition. An implicit **deny** is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 32.

Evaluation of an IP address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IP address match is found, the permit or deny statement is applied to that address and the remainder of the list is not evaluated.

Use the **no ip access-list** command to delete the access list.

The IPv4 standard access list is used to filter received and sent IPv4 routing information.

Examples

Example 1 - The following example of a standard access list allows only the three specified networks. Any IP address that does not match the access list statements will be rejected.

```
switchxxxxxx(config)# ip access-list 1 permit 192.168.34.0/24
switchxxxxxx(config)# ip access-list 1 permit 10.88.0.0/16
switchxxxxxx(config)# ip access-list 1 permit 10.0.0.0/8
```

Note: all other access is implicitly denied.

Example 2 - The following example of a standard access list allows access for IP addresses in the range from 10.29.2.64 to 10.29.2.127. All IP addresses not in this range will be rejected.

```
switchxxxxxx(config)# ip access-list apo permit 10.29.2.64/26
```

Note: all other access is implicitly denied.

Example 3 - To specify a large number of individual addresses more easily, you can omit the mask length if it is 32. Thus, the following two configuration commands are identical in effect:

```
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3
switchxxxxxx(config)# ip access-list 2aa permit 10.48.0.3/32
```

ipv6 access-list (IP standard)

The **ipv6 access-list** Global Configuration mode command defines an IPv6 standard list. The **no** format of the command removes the list.

Syntax

ipv6 access-list *access-list-name* {**deny**|**permit**} {*src-addr*[*/src-len*] | **any**}

no ipv6 access-list *access-list-name*

Parameters

- **access-list-name**—The name of the Standard IPv6 access list. The name may contain maximum 32 characters.
- **deny**—Denies access if the conditions are matched.
- **permit**—Permits access if the conditions are matched.
- **src-addr[/src-len] | any**— IPv6 prefix defined as an IPv6 address and length or any. The **any** value matches to all IPv6 addresses. If the *src-len* is not defined a value of 128 is applied. A value of *src-len* must be in interval 1-128.

Default Configuration

no access list

Command Mode

Global Configuration mode

User Guidelines

Use the **ipv6 access-list** command to configure IPv6 address filtering. Access lists are configured with **permit** or **deny** keywords to either permit or deny an IPv6 address based on a matching condition. An implicit **deny** is applied to address that does not match any access-list entry.

An access-list entry consists of an IP address and a bit mask. The bit mask is a number from 1 to 128.

Evaluation of an IPv6 address by an access list starts with the first entry of the list and continues down the list until a match is found. When the IPv6 address match is found, the permit or deny statement is applied to that address and the remainder of the list is not evaluated.

Use the **no ipv6 access-list** command to delete the access list.

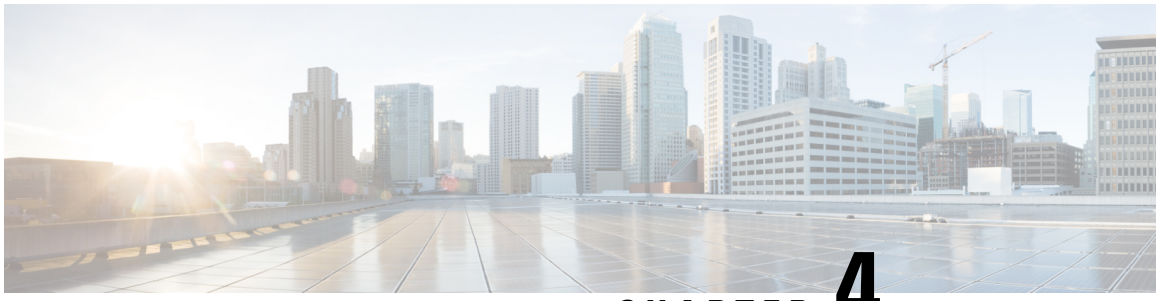
The IPv6 standard access list is used to filter received and sent IPv6 routing information.

Example

The following example of an access list allows only the one specified prefix: Any IPv6 address that does not match the access list statements will be rejected.

```
switchxxxxxx(config)# ipv6 access-list 1 permit 3001::2/64
```

Note: all other access implicitly denied.



CHAPTER 4

Address Table Commands

This chapter contains the following sections:

- bridge multicast filtering, on page 90
- bridge multicast mode, on page 90
- bridge multicast address, on page 91
- bridge multicast forbidden address, on page 92
- bridge multicast ip-address, on page 93
- bridge multicast forbidden ip-address, on page 94
- bridge multicast source group, on page 95
- bridge multicast forbidden source group, on page 96
- bridge multicast ipv6 mode, on page 97
- bridge multicast ipv6 ip-address, on page 98
- bridge multicast ipv6 forbidden ip-address, on page 99
- bridge multicast ipv6 source group, on page 100
- bridge multicast ipv6 forbidden source group, on page 101
- bridge multicast unregistered, on page 102
- bridge multicast forward-all, on page 103
- bridge multicast forbidden forward-all, on page 104
- bridge unicast unknown, on page 105
- show bridge unicast unknown , on page 105
- mac address-table static , on page 106
- clear mac address-table , on page 108
- mac address-table aging-time , on page 108
- port security, on page 109
- port security mode, on page 110
- port security max, on page 111
- port security routed secure-address, on page 112
- show mac address-table , on page 112
- show mac address-table count , on page 114
- show bridge multicast mode, on page 115
- show bridge multicast address-table, on page 116
- show bridge multicast address-table static, on page 118
- show bridge multicast filtering, on page 120
- bridge multicast unregistered, on page 120

- show ports security, on page 121
- show ports security addresses, on page 122
- bridge multicast reserved-address, on page 123
- show bridge multicast reserved-addresses, on page 124

bridge multicast filtering

To enable the filtering of Multicast addresses, use the **bridge multicast filtering** Global Configuration mode command. To disable Multicast address filtering, use the **no** form of this command.

Syntax

bridge multicast filtering

no bridge multicast filtering

Parameters

This command has no arguments or keywords.

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
```

bridge multicast mode

To configure the Multicast bridging mode, use the **bridge multicast mode** Interface (VLAN) Configuration mode command. To return to the default configuration, use the **no** form of this command.

Syntax

bridge multicast mode *{***mac-group** | **ipv4-group** | **ipv4-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 (VLAN) Configuration 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 mode, because there is no overlapping of IPv4 Multicast addresses in these modes.

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 mac-group on VLAN 2.

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast mode mac-group
```

bridge multicast address

To register a MAC-layer Multicast address in the bridge table and statically add or remove ports to or from the group, use the **bridge multicast address** Interface (VLAN) Configuration mode command. To unregister the MAC address, use the **no** form of this command.

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**—(Optional) Adds ports to the group.
- **remove**—(Optional) Removes ports from the group.
- **ethernet** *interface-list*—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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.

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 gi1/0/1-2
```

bridge multicast forbidden address

To forbid adding or removing a specific Multicast address to or from specific ports, use the **bridge multicast forbidden address** IInterface (VLAN) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (VLAN) Configuration 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 gi1/0/4 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 gi1/0/4
```

bridge multicast ip-address

To register IP-layer Multicast addresses to the bridge table, and statically add or remove ports to or from the group, use the **bridge multicast ip-address** IInterface (VLAN) Configuration mode command. To unregister the IP address, use the no form of this command.

Syntax

bridge multicast ip-address *ip-multicast-address* [[**add** | **remove**] {*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**—(Optional) Adds ports to the group.
- **remove**—(Optional) Removes ports from the group.
- ***interface-list***—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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 gi1/0/4
```

bridge multicast forbidden ip-address

To forbid adding or removing a specific IP Multicast address to or from specific ports, use the **bridge multicast forbidden ip-address** Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

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**—(Optional) Forbids adding ports to the group.
- **remove**—(Optional) Forbids removing ports from the group.
- **ethernet interface-list** —(Optional) 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**—(Optional) 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 (VLAN) Configuration 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 gi1/0/4 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 gi1/0/4
```

bridge multicast source group

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 **bridge multicast source group** Interface (VLAN) Configuration mode command. To unregister the source-group-pair, use the no form of this command.

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**—(Optional) Adds ports to the group for the specific source IP address.
- **remove**—(Optional) Removes ports from the group for the specific source IP address.
- **ethernet** *interface-list*—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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
```

bridge multicast forbidden source group

To forbid adding or removing a specific IP source address - Multicast address pair to or from specific ports, use the **bridge multicast forbidden source group** IInterface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

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**—(Optional) Forbids adding ports to the group for the specific source IP address.
- **remove**—(Optional) Forbids removing ports from the group for the specific source IP address.
- **ethernet** *interface-list*—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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 gi1/0/4 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
gi1/0/4
```

bridge multicast ipv6 mode

To configure the Multicast bridging mode for IPv6 Multicast packets, use the **bridge multicast ipv6 mode** Interface (VLAN) Configuration mode command. To return to the default configuration, use the no form of this command.

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 (VLAN) Configuration mode

User Guidelines

Use the **mac-group** mode when using a network management system that uses a MIB based on the Multicast MAC address.

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:

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

(*) In **ip-src-group** mode a match is performed on 4 bytes of the multicast address and 4 bytes of the source address. In the group address the last 4 bytes of the address are checked for match. In the source address the last 3 bytes and 5th from last bytes of the interface ID are examined.

(*) Note that (*,G) cannot be written to the 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
```

bridge multicast ipv6 ip-address

To register an IPv6 Multicast address to the bridge table, and statically add or remove ports to or from the group, use the **bridge multicast ipv6 ip-address** Interface (VLAN) Configuration mode command. To unregister the IPv6 address, use the **no** form of this command.

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**—(Optional) Adds ports to the group.
- **remove**—(Optional) Removes ports from the group.
- **ethernet** *interface-list*—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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 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 gi1/0/1-2
```

bridge multicast ipv6 forbidden ip-address

To forbid adding or removing a specific IPv6 Multicast address to or from specific ports, use the **bridge multicast ipv6 forbidden ip-address** Interface (VLAN) Configuration mode command. 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**—(Optional) Forbids adding ports to the group.
- **remove**—(Optional) Forbids removing ports from the group.
- **ethernet** *interface-list*—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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 gi1/0/4 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
 gi1/0/4
```

bridge multicast ipv6 source group

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 **bridge multicast ipv6 source group** Interface (VLAN) Configuration mode command. To unregister the source-group-pair, use the **no** form of this command.

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**—(Optional) Adds ports to the group for the specific source IPv6 address.
- **remove**—(Optional) Removes ports from the group for the specific source IPv6 address.
- **ethernet** *interface-list*—(Optional) 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*—(Optional) 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 (VLAN) Configuration 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
```

bridge multicast ipv6 forbidden source group

To forbid adding or removing a specific IPv6 source address - Multicast address pair to or from specific ports, use the **bridge multicast ipv6 forbidden source group** Interface (VLAN) Configuration mode command. To return to the default configuration, use the **no** form of this command.

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 (VLAN) Configuration 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 gi1/0/4 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 gi1/0/4
```

bridge multicast unregistered

To configure forwarding unregistered Multicast addresses, use the **bridge multicast unregistered** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, Port Channel) Configuration 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 gi1/0/1:

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  bridge multicast unregistered filtering
```

bridge multicast forward-all

To enable forwarding all multicast packets for a range of ports or port channels, use the **bridge multicast forward-all** Interface (VLAN) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (VLAN) Configuration mode

Example

The following example enables all Multicast packets on port gi1/0/4 to be forwarded.

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast forward-all add gi1/0/4
```

bridge multicast forbidden forward-all

To forbid a port to dynamically join Multicast groups, use the **bridge multicast forbidden forward-all** Interface (VLAN) Configuration mode command. To restore the default configuration, use the no form of this command.

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 (VLAN) Configuration 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 gi1/0/1 within VLAN 2.

```
switchxxxxxx(config)#  interface vlan 2
switchxxxxxx(config-if)#  bridge multicast forbidden forward-all add ethernet gi1/0/1
```

bridge unicast unknown

To enable egress filtering of Unicast packets where the destination MAC address is unknown to the device, use the **bridge unicast unknown** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, Port Channel) Configuration mode.

Example

The following example drops Unicast packets on gi1/0/1 when the destination is unknown.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  bridge unicast unknown filtering
```

show bridge unicast unknown

To display the unknown Unicast filtering configuration, use the **show bridge unicast unknown** Privileged EXEC mode command.

Syntax

show bridge unicast unknown [*interface-id*]

Parameters

interface-id—(Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel

Command Mode

Privileged EXEC mode

Example

Console # **show bridge unicast unknown**	
Port	Unregistered
--------	----------
gi1/0/1	Forward
gi1/0/2	Filter
gi1/0/3	Filter

mac address-table static

To add a MAC-layer station source address to the MAC address table, use the **mac address-table static** Global Configuration mode command. To delete the MAC address, use the **no** form of this command.

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**—(Optional) The permanent static MAC address. The keyword is applied by the default.
- **delete-on-reset**—(Optional)The delete-on-reset static MAC address.
- **delete-on-timeout**—(Optional)The delete-on-timeout static MAC address.
- **secure**—(Optional)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**—MAC address is saved until it is removed manually.
- **delete-on-reset**—MAC address is saved until the next reboot.

  delete-on-timeout—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**.

Example 1 - The following example adds two permanent static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b1 vlan 1 interface gi1/0/1
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
permanent
```

Example 2 - The following example adds a deleted-on-reset static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
delete-on-reset
```

Example 3 - The following example adds a deleted-on-timeout static MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface gi1/0/1
delete-on-timeout
```

Example 4 - The following example adds a secure MAC address:

```
switchxxxxxx(config)# mac address-table static 00:3f:bd:45:5a:b2 vlan 1 interface  gi1/0/1
 secure
```

clear mac address-table

To remove learned or secure entries from the forwarding database (FDB), use the **clear mac address-table** Privileged EXEC mode command.

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

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 gi1/0/1.

```
switchxxxxxx#  clear mac address-table secure interface gi1/0/1
```

mac address-table aging-time

To set the aging time of the address table, use the **mac address-table aging-time** Global configuration command. To restore the default, use the **no** form of this command.

Syntax

mac address-table aging-time *seconds*

no mac address-table aging-time

Parameters

seconds—Time is number of seconds. (Range:10-400)

Default Configuration

300

Command Mode

Global Configuration mode

Example

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

port security

To enable port security learning mode on an interface, use the **port security** Interface (Ethernet, Port Channel) Configuration mode command. To disable port security learning mode on an interface, use the **no** form of this command.

Syntax

port security [**forward** | **discard** | **discard-shutdown**] [**trap** *seconds*]

no port security

Parameters

- **forward**—(Optional) Forwards packets with unlearned source addresses, but does not learn the address.
- **discard**—(Optional) Discards packets with unlearned source addresses.
- **discard-shutdown**—(Optional) Discards packets with unlearned source addresses and shuts down the port.
- **trap** *seconds*—(Optional) 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 (Ethernet, Port Channel) Configuration mode

User Guidelines

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Port Security cannot be enabled on an interface if 802.1X authentication is already active on the interface.

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 gi1/0/1 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 gi1/0/4
switchxxxxxx(config-if)# port security mode lock
switchxxxxxx(config-if)# port security forward trap 100
switchxxxxxx(config-if)# exit
```

port security mode

To configure the port security learning mode, use the **port security mode** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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.
- **lock**— Secure mode without MAC learning.
- **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 (Ethernet, Port Channel) Configuration mode

User Guidelines

The default port mode is called regular. In this mode, the port allows unlimited learning of dynamic addresses.

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Example

The following example sets the port security mode to Lock for gi1/0/4.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# port security mode
lock

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

port security max

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 **port security max** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, Port Channel) Configuration mode

User Guidelines

The command may be used only when the interface in the regular (non-secure with unlimited MAC learning) mode.

Example

The following example sets the port to limited learning mode:

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# port security mode max
switchxxxxxx(config-if)# port security max 20
```

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

port security routed secure-address

To add a MAC-layer secure address to a routed port. (port that has an IP address defined on it), use the **port security routed secure-address** Interface (Ethernet, Port Channel) Configuration mode command. To delete a MAC address from a routed port, use the no form of this command.

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 (Ethernet, Port Channel) Configuration 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 gi1/0/1.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  port security routed secure-address 00:66:66:66:66:66
```

show mac address-table

To display entries in the MAC address table, use the **show mac address-table** Privileged EXEC mode command.

Syntax

show mac address-table [**dynamic** | **static** | **secure**] [**vlan** *vlan*] [**interface** *interface-id*] [**address** *mac-address]*

Parameters

- **dynamic**—(Optional) Displays only dynamic MAC address table entries.
- **static**—(Optional) Displays only static MAC address table entries.
- **secure**—(Optional) Displays only secure MAC address table entries.
- **vlan**—(Optional) Displays entries for a specific VLAN.
- **interface** *interface-id*—(Optional) Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **address** *mac-address*—(Optional) Displays entries for a specific MAC address.

Default Configuration

If no parameters are entered, the entire table is displayed.

Command Mode

Privileged 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 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	gi1/0/1	static
1	00:a1:b0:69:63:f3	gi1/0/2	dynamic
2	00:a1:b0:69:63:f3	gi1/0/3	dynamic
gi1/0/4	00:a1:b0:69:61:12	gi1/0/4	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       gi1/0/4
```

show mac address-table count

To display the number of addresses present in the Forwarding Database, use the **show mac address-table count** Privileged EXEC mode command.

Syntax

show mac address-table count [**vlan** *vlan* | **interface** *interface-id*]

Parameters

- **vlan** *vlan*—(Optional) Specifies VLAN.
- **interface-id** *interface-id*—(Optional) 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

Use the **show mac address-table count** command to display the Forwarding Database capacity (total number of entries), free entries (the number of entries that can still be used) and the consumed entries breakdown by type of entry. The following entry types are displayed:

- **Used Unicast** - Occupied Forwarding Database entries which are layer 2 MAC unicast addresses.
- **Used Multicast** - Occupied Forwarding Database entries which are layer 2 MAC Multicast addresses.
- **IPv4 hosts** - Occupied Forwarding Database entries which are IPv4 Layer 3 host entries.
- **IPv6 hosts** - Occupied Forwarding Database entries which are IPv6 Layer 3 host entries.
- **Secure** - The amount of the secure unicast entries.
- **Dynamic Unicast**- The amount of the dynamic unicast entries.
- **Static Unicast** - The amount of the static (configured by user) unicast entries.
- **Internal** - The amount of the internal entries. For example device own MAC address.

The Secure, Dynamic Unicast, Static Unicast and Internal entry types present further breakdown of the Used Unicast entries.

The total number of **consumed** entries is the aggregate value of the following entry types: Used Unicast; Used Multicast ;IPv4 hosts ;IPv6 hosts .

If the **Interface** parameter is used the command will display only the following entry types: Used Unicast, secure, Dynamic Unicast, Static Unicast and Internal.

Example 1 - The following example displays the number of entries present in forwarding table for the entire device:

```
switchxxxxxx#  show mac address-table count
This may take some time.
Capacity         : 16384
Free               : 16378
Used unicast     : 5
Used multicast   : 1
Used IPv4 hosts  : 1
Used IPv6 hosts  : 1 (each IPv6 host consumes 2 entires in MAC address table)
Secure           : 0
Dynamic unicast  : 2
Static unicast   : 2
Internal         : 1
console#
```

Example 2 - The following example displays the number of entries present in forwarding table for a specific device interface.

```
switchxxxxxx#  show mac address-table count interface gi1/0/1
This may take some time.
Capacity         : 16384
Free               : 16378
Used unicast     : 5
Secure           : 0
Dynamic  unicast : 2
Static unicast   : 2
Internal         : 0
console#
```

show bridge multicast mode

To display the Multicast bridging mode for all VLANs or for a specific VLAN, use the **show bridge multicast mode** Privileged EXEC mode command.

Syntax

show bridge multicast mode [*vlan vlan-id*]

Parameters

vlan *vlan-id*—(Optional) Specifies the VLAN ID.

Command Mode

Privileged 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-GROUP	IPv4-SRC-GROUP	IPv6-SRC-GROUP	IPv6-SRC-GROUP

show bridge multicast address-table

To display Multicast MAC addresses or IP Multicast address table information, use the **show bridge multicast address-table** Privileged EXEC mode command.

Syntax

show bridge multicast address-table [**vlan** *vlan-id*]

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *mac-multicast-address*] [**format** {**ip** | **mac**}]

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *ipv4-multicast-address]* [**source** *ipv4-source-address*]

show bridge multicast address-table [**vlan** *vlan-id*] [**address** *ipv6-multicast-address*] [**source** *ipv6-source-address*]

Parameters

- **vlan-id** *vlan-id*—(Optional) Display entries for specified VLAN ID.
- **address**—(Optional) Display entries for specified Multicast address. The possible values are:

  mac-multicast-address—(Optional) Specifies the MAC Multicast address.

  ipv4-multicast-address—(Optional) Specifies the IPv4 Multicast address.

  ipv6-multicast-address—(Optional) Specifies the IPv6 Multicast address.
- **format**—(Optional) Applies if mac-multicast-address was selected. In this case either MAC or IP format can be displayed. 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** —(Optional) Specifies the source address. The possible values are:

  ipv4-address—(Optional) Specifies the source IPv4 address.

  ipv6-address—(Optional) 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

Privileged 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.

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      gi1/0/4
```

Multicast address table for VLANs in IPv4-GROUP bridging mode:

```
Vlan    MAC Address         Type             Ports
---- -----------------    --------------     -----
1      224.0.0.251         Dynamic           gi1/0/2
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     gi1/0/1
Forbidden ports for Multicast addresses:
Vlan  Group Address  Source Address   Ports
---- --------------- --------------- -------
8    239.2.2.2       *               gi1/0/4
8    239.2.2.2       1.1.1.11        gi1/0/4
Multicast address table for VLANs in IPv6-GROUP bridging mode:
VLAN  IP/MAC Address   Type      Ports
---- ----------------- --------- ---------------------
8    ff02::4:4:4       Static    gi1/0/1-2, gi1/0/3, Po1
Forbidden ports for Multicast addresses:
VLAN  IP/MAC Address   Ports
---- ----------------- -----------
8    ff02::4:4:4       gi1/0/4
Multicast address table for VLANs in IPv6-SRC-GROUP bridging mode:
Vlan  Group Address  Source address  Type     Ports
---- --------------- --------------- -------- ------------------
8    ff02::4:4:4     *               Static   gi1/0/1-2,gi1/0/3,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     *                  gi1/0/4
8    ff02::4:4:4     fe80::200:7ff:f    gi1/0/4
                     e00:200
```

show bridge multicast address-table static

To display the statically-configured Multicast addresses, use the **show bridge multicast address-table static** Privileged EXEC mode command.

Syntax

show bridge multicast address-table static [**vlan** *vlan-id*] [**all**]

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *mac-multicast-address*] [**mac**| **ip**]

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *ipv4-multicast-address*] [**source** *ipv4-source-address*]

show bridge multicast address-table static [**vlan** *vlan-id*] [**address** *ipv6-multicast-address*] [**source** *ipv6-source-address*]

Parameters

- **vlan** *vlan-id*—(Optional) Specifies the VLAN ID.
- **address**—(Optional) Specifies the Multicast address. The possible values are:

  mac-multicast-address—(Optional) Specifies the MAC Multicast address.

  ipv4-multicast-address—(Optional) Specifies the IPv4 Multicast address.

  ipv6-multicast-address—(Optional) Specifies the IPv6 Multicast address.
- **source**—(Optional) Specifies the source address. The possible values are:

  ipv4-address—(Optional) Specifies the source IPv4 address.

  ipv6-address—(Optional) Specifies the source IPv6 address.

Default Configuration

When **all/mac/ip** is not specified, all entries (MAC and IP) will be displayed.

Command Mode

Privileged 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       gi1/0/1, gi1/0/2

Forbidden ports for multicast addresses:

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

IPv4-GROUP Table

Vlan        IP Address           Ports
----        ----------           --------
1           231.2.2.3            gi1/0/1, gi1/0/2
19          231.2.2.8            gi1/0/2-3

Forbidden ports for multicast addresses:

Vlan        IP Address           Ports
----        ----------           --------
1           231.2.2.3            gi1/0/4
19          231.2.2.8            gi1/0/3

IPv4-SRC-GROUP Table:

Vlan        Group Address        Source address       Ports
----        ---------------      ---------------      ------

Forbidden ports for multicast addresses:

Vlan        Group Address        Source address       Ports
----        ---------------      ---------------      ------

IPv6-GROUP Table

Vlan        IP Address           Ports
----        -----------------    ---------
191         FF12::8              gi1/0/1-4

Forbidden ports for multicast addresses:

Vlan        IP Address           Ports
----        -----------------    ---------
11          FF12::3              gi1/0/4
191         FF12::8              gi1/0/4

IPv6-SRC-GROUP Table:

Vlan        Group Address        Source address       Ports
----        ---------------      ---------------      ------
192         FF12::8              FE80::201:C9A9:FE40:8988 gi1/0/1-4

Forbidden ports for multicast addresses:

Vlan        Group Address        Source address       Ports
----        ---------------      ---------------      ------
192         FF12::3              FE80::201:C9A9:FE40:8988 gi1/0/4
```

show bridge multicast filtering

To display the Multicast filtering configuration, use the **show bridge multicast filtering** Privileged EXEC mode command.

Syntax

show bridge multicast filtering *vlan-id*

Parameters

vlan-id—Specifies the VLAN ID. (Range: Valid VLAN)

Default Configuration

None

Command Mode

Privileged 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
gi1/0/1	Forbidden	Filter
gi1/0/2	Forward	Forward(s)
gi1/0/3	-	Forward(d)

bridge multicast unregistered

To configure forwarding unregistered Multicast addresses, use the **bridge multicast unregistered** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet, Port Channel) Configuration 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 gi1/0/1:

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  bridge multicast unregistered filtering
```

show ports security

To display the port-lock status, use the **show ports security** Privileged EXEC mode command.

Syntax

show ports security [*interface-id* | **detailed**]

Parameters

- ***interface-id***—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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
------- --------    ---------   ------    ---      -------  --------
gi1/0/1
       Enabled      Max-       Discard     3       Enabled  100
                    Addresses
gi1/0/2
      Disabled     Max-         -          28        -        -
                   Addresses
gi1/0/3
     Enabled       Lock      Discard      8       Disabled   -
```

The following table describes the fields shown above.

Description
The port number.
The port security status. The possible values are: Enabled or Disabled.
The action taken on violation.
The maximum number of addresses that can be associated on this port in the Max-Addresses mode.
The status of SNMP traps. The possible values are: Enable or Disable.
The minimum time interval between consecutive traps.

show ports security addresses

To display the current dynamic addresses in locked ports, use the **show ports security addresses** Privileged EXEC mode command.

Syntax

show ports security addresses [*interface-id* | **detailed**]

Parameters

- ***interface-id***—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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
-------     --------    --------    ----------  ----------
gi1/0/1     Disabled    Lock        0           10
gi1/0/2     Disabled    Lock        0           1
gi1/0/3     Disabled    Lock        0           1
gi1/0/4     Disabled    Lock        0           1
...
```

bridge multicast reserved-address

To define the action on Multicast reserved-address packets, use the **bridge multicast reserved-address** Global Configuration mode command. To revert to default, use the **no** form of this command.

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*—(Optional) Specifies that the packet type is Ethernet v2 and the Ethernet type field (16 bits in hexadecimal format). (Range: 0x0600–0xFFFF)
- **llc** *sap*—(Optional) Specifies that the packet type is LLC and the DSAP-SSAP field (16 bits in hexadecimal format). (Range: 0xFFFF)
- **llc-snap** *pid*—(Optional) 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(config)# bridge multicast reserved-address 00:3f:bd:45:5a:b1
```

show bridge multicast reserved-addresses

To display the Multicast reserved-address rules, use the **show bridge multicast reserved-addresses** Privileged EXEC mode command.

Syntax

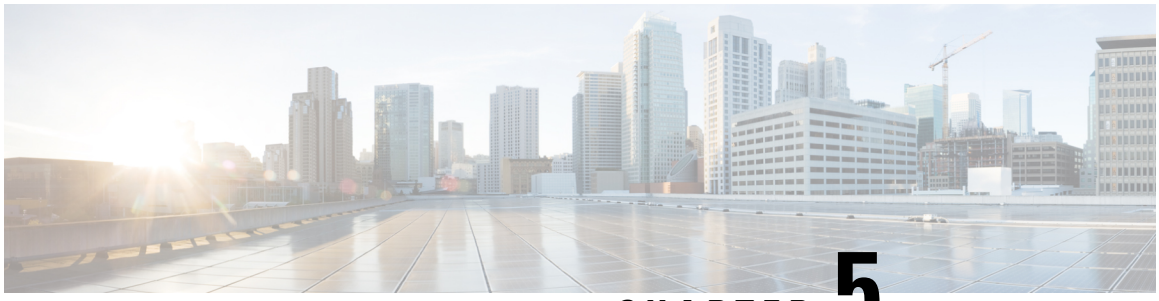
show bridge multicast reserved-addresses

Command Mode

Privileged 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
```



CHAPTER 5

AAA Commands

This chapter contains the following sections:

- aaa authentication login, on page 126
- aaa authentication enable, on page 127
- login authentication, on page 128
- enable authentication, on page 129
- ip http authentication, on page 130
- show authentication methods, on page 131
- aaa authorization commands, on page 131
- aaa authorization config-commands, on page 133
- aaa authorization console, on page 134
- authorization command, on page 135
- show authorization methods, on page 136
- login block-for, on page 137
- login delay, on page 138
- login quiet-mode access-class, on page 139
- show login, on page 140
- show login failures, on page 141
- clear login failures, on page 142
- clear login quiet-mode, on page 142
- password, on page 143
- enable password , on page 144
- service password-recovery, on page 146
- username , on page 147
- show users accounts, on page 149
- aaa accounting commands, on page 150
- accounting commands, on page 151
- show accounting methods, on page 151
- passwords complexity keyboard-pattern, on page 152
- aaa accounting login start-stop, on page 153
- aaa accounting dot1x , on page 154
- aaa accounting update periodic, on page 156
- show accounting, on page 156
- passwords complexity, on page 157

• passwords aging, on page 158
• password complexity history, on page 159
• show passwords configuration, on page 159

aaa authentication login

Use the **aaa authentication login** Global Configuration mode command to set one or more authentication methods to be applied during login. Use the **no** form of this command to restore the default authentication method.

Syntax

aaa authentication login [**authorization**] {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*}

Parameters

- **authorization**—Specifies that authentication and authorization are applied to the given list. If the keyword is not configured, then only authentication is applied to the given list.
- **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**.

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.

Note. If authorization is enabled for login and the switch receives from a TACACS+ server user level 15, then the enable command is not required and if received level 1 the enable command is required.

The **no aaa authentication login** *list-name* command 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
```

aaa authentication enable

The **aaa authentication enable** Global Configuration mode command sets one or more authentication methods for accessing higher privilege levels. To restore the default authentication method, use the **no** form of this command.

Syntax

aaa authentication enable [**authorization**] {**default** | *list-name*} *method* [*method2...*]}

no aaa authentication enable {**default** | *list-name*}

Parameters

- **authorization**—Specifies that authentication and authorization are applied to the given list. If the keyword is not configured, then only authentication is applied to the given list.
- **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.

Keyword	Description
line	Uses the line password 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

No Authentication lists exist by default.

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.

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
```

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 the **aaa authentication login** command.

Default Configuration

default

Command Mode

Line Configuration Mode

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 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
```

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

default.

Command Mode

Line Configuration Mode

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
```

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 [**login-**authorization] *method1* [*method2...*]

no ip http authentication aaa login-authentication

Parameters

- **login-**authorization—Specifies that authentication and authorization are applied. If the keyword is not configured, then only authentication is applied.
- ***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
```

show authentication methods

The **show authentication methods** Privileged EXEC mode command displays information about the authentication methods.

Syntax

show authentication methods

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
Consl_Login(with authorization): Line, None
Enable Authentication Method Lists
----------------------------------
Default: Radius, Enable
Consl_Enable(with authorization): Enable, None
```

.

Line	Login Method List	Enable Method List
Console	Consl_Login	Consl_Enable
Telnet	Default	Default
SSH	Default	Default

```
HTTP, HHTPS: Radius, local
Dot1x: Radius
```

aaa authorization commands

Use the aaa authorization commands Global Configuration mode command to create a method list that can be used for command authorization, use the no command to delete a method list.

Syntax

aaa authorization commands {default | *list-name} method [method2...]}*

no aaa authorization commands {default | *list-name}*

Parameters

- *privilege-level* - specifies the privilege level of the commands that the authorization list will address:
  - 1 – Defines a commands authorization method list for level 1 commands.
  - 7 - Defines a commands authorization method list for level 7 commands.
  - 15 - Defines a commands authorization method list for level 15 commands.
- {**default** | Uses the listed commands authorization methods that follow this argument as the default method list.
- *list-name*: Specifies a name for the list of commands authorization methods. (Length:1–20 characters)
- *method* [*method2...*]—Specifies a list of methods that the commands authorization algorithm tries, in the given sequence. The additional authorization methods are used only if the previous method is not active, not if it rejected a command. Select one or more methods from the following list:

Keyword	Description
none	Commands authorization is not required.This method is usually used as a fall back if the previous methods are not reachable
if-authenticated	Specifies that the commands of the specific level are authorized if the user has been authenticated to that level. This method is usually used as fall back if the previous methods are not reachable.
local	Specifies that the local database should be used for commands authorization. This method is usually used as a fall back if the previous methods are not reachable.
tacacs	Uses the list of all TACACS+ servers for commands authorization.

Default Configuration

The Default method list exists, using none as the only method

Command Mode

Global configuration mode

User Guidelines

Use the aaa authorization commands command to specify a method list for authorizing commands executed by the user. If the method list includes more than one method, then the methods are used in the order specified in the command. A secondary method will be used only if the previous method is un-reachable.

Command authorization will not be applied to a configuration mode command unless the aaa authorization config-commands is also configured on the device.

Use the no form of the command to return the default method list to its default (none is the only method), or to delete a named method list that was created by the user.

If local is defined as a method the commands will be authorized based on the credentials provided by the user and according to their privilege level. This means that a level 1 user will be able to execute all of the level 1 commands and a level 15 user will be able to execute all of the level 15 commands. If the credentials used for login are not part of the local database then execution for all of the commands will fail. This method is usually used as a backup in case the main method (for example tacacs) is not reachable. It prevents command execution lockout in this case.

The none and if-authenticated are also used usually as backup method. If none is defined as a method – then the commands will always be authorized. The if-authenticated method functionality is similar to the none method functionality. However if the user did not provide any credentials when login in (for example authentication and authorization method list were none), then if none is defined as a command authorization list all commands will be authorized, and if the if-authenticated method is used all commands will be denied (since the user was not authenticated).

In order to activate a method list it needs to be applied to a management interface (console, SSH or telnet) using the authorization commands line configuration mode command.

Example

The following example configures an authorization method list for level 15 commands. The authorization requests are sent to the list of the TACACS+ servers. If the TACACS+ servers do not respond, then the commands are still authorized (due to the none method).

```
switchxxxxxx(config)# aaa authorization commands 15 auth_commands15 tacacs
none
```

aaa authorization config-commands

Use the aaa authorization config-commands to define that configuration commands require authorization. Use the no form of the command to return to default settings.

Syntax

aaa authorization config-commands

no aaa authorization config-commands

Parameters

N/A

Default

By default, configuration mode commands do not require authorization.

User Guidelines

This command is used to define that configuration commands require authorization. If the **aaa authorization config-commands** command is not configured then configuration commands do not require authorization, even if the **aaa authorization commands** command was defined.

If the **aaa authorization config-commands** command configured then also configuration commands require authorization. The configuration commands will be authorized using the active level 15 or level 7 method list.

Example

The following example enables command authorization for Configuration mode CLI commands.

```
switchxxxxxx(config)# aaa authorization config-commands
```

aaa authorization console

Use the aaa authorization console global mode command to activate Command Authorization method list that were applied to the console interface. Use the no form of the command to de-activate methods applied to the console interface.

Syntax

aaa authorization console

no aaa authorization console

Parameters

N/A

Default

Command Authorization method list that were applied to the console interface are not active.

Command Mode

Global Configuration mode

User Guidelines

Use the **aaa authorization console** command to activate Command Authorization method list that were applied to the console interface. Without this command methods that were applied to the console interface (command) will be part of the device configuration but will not be active.

Use the **no** to de-activate Command Authorization method list that were applied to the console

authorization command

The **authorization commands** Line Configuration Mode command enables a commands authorization method list for a management line. Use the **no** form of this command to restore the default commands authorization method list.

Syntax

authorization commands *privilege-level* {**default**| *list-name*}

no authorization commands

Parameters

- *privilege-level* - specifies the privilege level of the commands that the authorization list will address:
  - 1 – Defines a commands authorization method list for level 1 commands.
  - 7 - Defines a commands authorization method list for level 7 commands.
  - 15 - Defines a commands authorization method list for level 15 commands.
- {**default** | Applies the default list defined with the command **aaa authorization commands**.
- *list-name*: Applies the specified named list created with the commands **aaa authorization methods**.

Default Configuration

The default method list is applied to each of the command levels.

Command Mode

Line Configuration Mode

User Guidelines

Use the command authorization commands to enable a commands authorization method list to a management line (console, telnet or SSH). The commands authorization method list are enabled per command level. A named authorization list can be specified only if it was previously created using the command **aaa authorization commands**.

Use the command **no authorization commands** to remove a named method list and enable the **default** method list for the level that was specified in the command.

Command authorization method list applied to the console interface will be active only after the command **aaa authorization console** is configured. If a method list is applied to the console interface and the command **aaa authorization console** is not configured, the command will be accepted but the following notification will be displayed: “Authorization without the global command 'aaa authorization console' is useless”

Examples

Example 1 - The following example enables the defau

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# authorization commands 1 default
```

Example 2 - The following example enables the auth_comm15 commands authorization named list for the level 15 command configured on the console interface.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# authorization commands 15 auth_comm15
```

show authorization methods

Use the **show authorization methods** Privileged EXEC mode command to display the Command Authorization methods and the management interfaces to which they were applied.

Syntax

show authorization methods

Parameters

N/A

Defaults

N/A

Example

Example 1-

```
switchxxxxxx# show authorization methods
commands level 1 Authorization Method Lists
---------------------------------
Default : Tacacs None
comAuth1 : Tacacs Local
commands level 7 Authorization Method Lists
---------------------------------
Default : Tacacs None
comAuth7 : Tacacs Local
commands level 15 Authorization Method Lists
---------------------------------
Default : Tacacs None
comAuth15 : Tacacs Local
Console Authorization: enabled
Configuration Authorization: enabled
Line Commands level 1 Commands level 7 Commands level 15
Method List Method List Method List
------- ----------------- ---------------- ------------------
Console Default comAuth7 Default
Telnet comAuth1 Default Default
SSH Default Default comAuth15
```

login block-for

Login Block-for

Use the following global configuration mode command to configure a quiet mode period followed specified number of failed login attempts. Use the no form of command to return to default settings:

Syntax

login block-for seconds **attempts** tries **within** seconds

no login block-for

Parameters

- **Block for seconds** - Duration (in seconds) of quiet mode period (the time in which login attempts are denied) (range 1 - 65535 (18 hours) seconds).
- **attempts** tries - The number of failed login attempts that triggers the quiet mode period (range 1-100).
- **within** seconds - Duration of time (in seconds) in which the number of failed login attempts must be made before the quiet mode period is triggered (range 1 - 3600 (1 hour) seconds).

Default Configuration

Quiet mode is not configured on device.

Command Mode

Global Configuration mode.

User Guidelines

If the specified number of connection attempts fails (**attempt** tries) within a specified time (**within** seconds), the device will not accept any additional login attempts for a specified period of time (**block-for** seconds).

During the quiet-mode period, management connections to device are restricted by the quiet-mode access-class which allows only the specified connections (command **login quiet-mode access-class**). For devices that support a console connection the “console_only” management access-list is used as the default quiet-mode access-class. In this case, all login attempts over the network (Telnet, SSH, SNMP, HTTP or HTTPS) are denied during the quiet-mode period.

This command can be configured only if a quiet-mode access-class (default or user defined) is configured – see “login quiet-mode access-class”

If the **login block-for** command is already configured on device and the command is reconfigured with new parameters during the “watch period” – then the current count will be terminated, and a new count will begin using new parameters. The Command is rejected if configured during login attack quiet-mode period.

The **no** form of command disables the feature and terminates the quiet mode period, if active.

Examples

Example 1 - The following example shows how to block all login requests for 180 seconds if 18 failed login attempts are exceeded within 180 seconds:

```
switchxxxxxx(config)# login block-for 180 attempts 18 within 180
```

Example 2 -The following example displays an attempt to configure command during device quiet mode period:

```
switchxxxxxx(config)# login block-for 18 attempts 8 within 50
```

Cannot configure login block-for setting while device is in Quiet-Mode.

Example 3 - The following example displays an failure to configure command. Failure reason: quiet-mode access class (default or user defined) is not configured:

```
switchxxxxxx(config)# login block-for 770 attempts 7 within 613
```

Cannot configure login block-for setting since quiet-mode access-class is not configured.

login delay

Use the **login delay** Global Configuration mode command to configure a delay in device response to a failed login attempts. Use the no form of this command to return to the default setting.

Syntax

login delay seconds

no login delay

Parameters

- seconds - The delay (in seconds) that is imposed between failed login attempts (range 1-10 seconds).

Default Configuration

By default, login delay is disabled.

Command Mode

By default, login delay is disabled.

User Guidelines

The login delay command introduces a delay in device response following a failed login attempt (HTTP, HTTPS, Telnet, SSH and SNMP). The delay provides better protection from possible dictionary attacks.

Examples

Example 1 - The following example sets a delay of 5 seconds following a failed login attempt:

```
switchxxxxxx(config)# login delay 5
```

login quiet-mode access-class

Use the login quiet-mode access-class Global Configuration mode command to to specify a management access control list (MACL) that will be applied when the device transitions to the login quiet-mode. Use the no form of this command to return to the default setting.

Syntax

login quiet-mode access-class name

no login quiet-mode access-class

Parameters

- ***name*** – the name of the management ACL to apply on the device while in login quiet mode.

Default Configuration

By default, the "console-only" management access list is applied as the default quiet-mode access-class. For devices that do not support console - the quiet-mode access-class has no default.

Command Mode

Global configuration mode.

User Guidelines

Use the **login quiet-mode access-class** command to allow selective hosts access to the device management during a login quiet period. Access is allowed based on the specified Management ACL. The management access list needs to be created prior to configuring this command using the management access-list command.

This settings provides the ability to grant access to a client or list of clients even during a quiet-mode period. On devices that support a console connection the "console-only" management access-list is applied by default during a quiet-mode period, meaning all network login connections (telnet, SSH, SNMP, HTTP, HTTPS) are denied, while a connection from the console is allowed. On devices that do not support a console there is no default access-class and the login block-for command cannot be configured if user did not first define a quiet-mode access-class.

The command is rejected if it is configured during a quiet-mode period.

The no form of the command returns quiet-mode access-class to the default setting. On devices without a console the no command cannot be applied if login block-for command is configured.

Examples

Example 1 - The following example shows how to configure the device to accept connection during quiet mode period based on quiet-acl management access list:

```
switchxxxxxx(config)# login quiet-mode access-class quiet-acl
```

show login

Use the following privileged exec mode command to display login setting and status:

Syntax

show login

Parameters

N/A

Default Configuration

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This command displays setting and status related to commands **login delay**, **Login block-for and login quiet-mode access-class**.

Examples

Example 1 - The following example shows output if no login settings have been applied or changed:

```
switchxxxxxx# show login
Login delay: disabled
Login Attacks watch: disabled
Quiet-Mode access list: console-only (the default)
```

Example 2 - The following example shows the show login command output where the user set the login delay to 5 seconds, configured a login block period and the device is not in quiet-mode:

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for 60
seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: inactive
Watch Window remaining time: 44 seconds.
Present login failure count: 3.
```



Note Login failure count is counted from the earliest failed login that is still valid (within a watching windows)

Example 3 - The following example shows output where user set login delay to 5 seconds, configured a login block period and device is in quiet mode:

```
switchxxxxxx# show login
Login delay: 5 second
```

```
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for 60
seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: active (time remaining: 20 seconds)
```

show login failures

Use the following privileged exec mode command to display information on failed login attempts:

Syntax

Show login failures

Parameters

NA

Default Configuration

NA

Command Mode

Privileged EXEC mode

User Guidelines

This command displays information on last 50 failed login attempts. Information includes the username provided in the failed attempt (if provided as part of attempt), source IP used in failed attempt, service requested in the failed attempt, the number of failed attempts for this connection and the time stamp of last failed attempt for this connection. Entries are sorted from the newest time stamp to the oldest.

Examples

```
switchxxxxxx#  show login failures
```

Information about last 50 login failure's with the device.

Username	Source IP	Service	Count	TimeStamp
————	————	————	————	————
ffff	10.5.44.25	telnet	3	00:01:23 edt Wed Jul 7 2021
fff	10.5.44.25	telnet	4	08:37:08 edt Thu Jul 8 2021
bb	10.5.44.25	ssh	2	00:17:59 edt Wed Jul 7 2021
fff	10.5.44.25	ssh	2	00:20:37 edt Wed Jul 7 2021

Username	Source IP	Service	Count	TimeStamp
ffff	10.5.44.25	ssh	2	00:21:12 edt Wed Jul 7 2021
aaaa	fe80::1111	ssh	2	00:21:26 edt Wed Jul 7 2021
	10.5.44.25	telnet	3	00:38:14 edt Wed Jul 7 2021
aaa	10.5.44.22	telnet	1	08:37:16 edt Thu Jul 8 2021
555	10.5.44.23	telnet	1	08:37:26 edt Thu Jul 8 2021

clear login failures

Use the following privileged exec mode command to clear login failure database:

Syntax

clear login failures

Parameters

NA

Default Configuration

NA

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to clear all entries in login failure database (command **show login failures**).

Examples

```
switchxxxxxx#  clear login failures
```

clear login quiet-mode

Use the following privileged exec mode command to immediately terminate an active quiet-mode period:

Syntax

clear login quiet-mode

Parameters

NA

Default Configuration

NA

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to terminate an active quiet-period, without disabling the feature (command **login block-for**). Quiet mode period will be terminated even if the quiet mode period timer did not expire.

Examples

```
switchxxxxxx#  clear login quiet-mode
11-Aug-2021 10:33:12 :%ABC-I-XXX: Quiet-Mode is OFF, terminated by user
```

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 {*unencrypted-password* [**method** *hash-method***]** | *encrypted-password* **encrypted**}

password generate-password [**method** hash-method]

no password

Parameters

- ***unencrypted-password***—The authentication password for the user. (Range: 1–64)
- [**method** *hash-method***]** — (optional) specifies the method used for encrypting the clear-text password. Supported values:
  - **sha512** - PBKDF2 encryption with HMAC using the SHA512 as the underlying Hashing Algorithm. This is the default method if the **method** parameter is not specified.
- **encrypted** encrypted-password—Specifies that the password is encrypted and hashed using a salt. Use this keyword to enter a password that is already encrypted (for instance, a password that was copied from the configuration file of another device). The *encrypted-password* is specified in the format of *$<type>$<salt>$<encrypted-password >*, where:
  - **<*type*>** - is an integer value that indicates the type of hash algorithm used to generate the hash

- **<salt>** - The base64 encoding of the 96 bits used for salt (length – 16 bytes)
- ***<encrypted-password>*** - The base64 encoding of the encrypted hash output (length - 86 bytes)

Default Configuration

No password is defined.

Command Mode

Line Configuration Mode

User Guidelines

The *unencrypted-password* must comply to password complexity requirements.

If the **generate-password** option is selected, the user does not need to input a password. Instead, the device will automatically generate a random based password suggestion. This suggestion will be displayed to the user, and the user will be presented with an option to accept or reject the proposed password. If user selected to accept the proposed password, then the specified username with this password (in encrypted format) will be added to device configuration file. If user rejects the proposed password then a new command needs to be entered by the user.

Example

Example 1 -The following example specifies the password 'secreT123!' on the console line.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secreT123!
```

Example 2 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to accept the proposed password.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use."
```

Example 3 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to reject the proposed password.

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
"Auto generated password rejected by user. Password configuration is not added to
device configuration"
```

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.

Syntax

enable password [**level** *privilege-level*] {[**method** *hash-method***]** *unencrypted-password* | **encrypted** encrypted-password}

no enable password [**level** *privilege-level*]

Parameters

- **level** privilege-level—Level for which the password applies. If not specified, the level is 15. (Range: 1–15)
- [**method** *hash-method***]** — (optional) specifies the method used for encrypting the clear-text password. Supported values:
  - **sha512** - PBKDF2 encryption with HMAC using the SHA512 as the underlying Hashing Algorithm. This is the default method if the **method** parameter is not specified.
- *unencrypted-password*—Password for this level. (Range: 0–159 chars)
- **encrypted** encrypted-password—Specifies that the password is encrypted and hashed using a salt. Use this keyword to enter a password that is already encrypted (for instance, a password that was copied from the configuration file of another device). The *encrypted-password* is specified in the format of *$<type>$<salt>$<encrypted-password >*, where:
  - **<*type*>** - is an integer value that indicates the type of hash algorithm used to generate the hash
  - **<salt>** - The base64 encoding of the 96 bits used for salt (length – 16 bytes)
  - **<*encrypted-password*>** - The base64 encoding of the encrypted hash output (length - 86 bytes)

Default Configuration

Default for **level** is 15.

Command Mode

Global Configuration mode

User Guidelines

The *unencrypted-password* must comply to password complexity requirements

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. The administrator is required to use the **encrypted** keyword only when actually entering an encrypted keyword.

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.

The administrator is required to use the **encrypted** keyword only when actually entering an encrypted keyword.

If the **generate-password** option is used, instead of entering a password the user will be presented with a randomly generated password suggestion. This suggestion will comply with all current password strength settings

The user will be given the choice to accept or reject the proposed password. If the user elects to accept the password, then this password will be added for the configured enable level (in encrypted format) in the configuration file.

If the user rejects the password suggestion, the command will need to be entered again to configure this enable level.

Example

Example 1 - The command sets a password that has already been encrypted. It will be copied to the configuration file just as it is entered. To login to device using this password, the user must know its unencrypted form.

```
switchxxxxxx(config)# enable password encrypted
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc7
2hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

Example 2 - The command sets an unencrypted password for level 1 (it will be encrypted in the configuration file).

```
switchxxxxxx(config)# enable password level 1 let-me-In
```

Example 3 - The command in this example includes the **generate-password** key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to **accept** the proposed password.

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use"
```

Example 4 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to rejects the proposed password.

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
"Auto generated password rejected by user. Password configuration is not added to
device configuration"
```

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

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.

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.
```

username

Use the **username** Global Configuration mode command to create or edit a username based user authentication account. Use the **no** form to remove a user account.

Syntax

username name {[**method** *hash-method*] **password** {*unencrypted-password* | {**encrypted** encrypted-password}} | {**privilege** privilege-level {[**method** *hash-method*] *unencrypted-password* | {**encrypted** encrypted-password}}}}

username name {[**method** hash-method] **generate-password** | {**privilege** privilege-level{[**method** hash-method] **generate-password**}

no username name

Parameters

- ***name***—The name of the user. (Range: 1–20 characters)

- [**method** *hash-method*] — (optional) specifies the method used for encrypting the clear-text password. Supported values:
  - **sha512** - PBKDF2 encryption with HMAC using the SHA512 as the underlying Hashing Algorithm. This is the default method if the **method** parameter is not specified.
- **password**—Specifies the password for this username.
- unencrypted-password—The authentication password for the user. (Range: 1–64)
- **encrypted** encrypted-password—Specifies that the password is encrypted and hashed using a salt. Use this keyword to enter a password that is already encrypted (for instance, a password that was copied from the configuration file of another device). The *encrypted-password* is specified in the format of *$<type>$<salt>$<encrypted-password >*, where:
  - ***<type>*** - is an integer value that indicates the type of hash algorithm used to generate the hash.
  - ***<salt>*** - The base64 encoding of the 96 bits used for salt (length – 16 bytes)
  - ***<encrypted-password>*** - The base64 encoding of the encrypted hash output (length - 86 bytes)
- **generate-password** - The device automatically generates a random based password suggestion. The user has an option to accept or reject the proposed password.
- **privilege** privilege-level —User account privilege level. If not specified the level is 1. (Range: 1–15).

Default Configuration

No user is defined.

Command Mode

Global Configuration mode

Usage Guidelines

The *unencrypted-password* must comply to password complexity requirements.

If the generate-password option is used, instead of entering a password the user will be presented with a randomly generated password suggestion. This suggestion will comply with all current password strength settings. The user will be given the choice to accept or reject the proposed password. If the user elects to accept the password, then this password will be added for the configured user name (in encrypted format) in the configuration file.

If the user rejects the password suggestion, the command will need to be entered again to configure this user.

The knowledge of the current password is required if the user requests to modify the password of the account used to login to the current session (while maintaining the current username). The user will be prompted to provide the current password in clear-text format. The password change will succeed only if the user correctly provided the current password.

The last level 15 user cannot be removed and cannot be a remote user

Example

Example 1- Sets an unencrypted password for user tom (level 15). It will be encrypted in the configuration file.

```
switchxxxxxx(config)# username tom password 1234Ab$5678
```

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
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc72hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

Example 3 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to accept the proposed password.

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use."
```

Example 4 - The command in this example includes the generate-password key word. in this case the device will propose a randomly generated password to be used. in the example below the user selects to reject the proposed password.

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
"Auto generated password rejected by user. Password configuration is not added to
device configuration."
```

show users accounts

The **show users accounts** Privileged EXEC mode command displays information about the users local database.

Syntax

show users accounts

Command Mode

Privileged EXEC mode

Example

The following example displays information about the users local database:

```
switchxxxxxx# show users accounts

Username        Privilege       Password
--------        ---------       Expiry date
Bob             15              ----------
Robert          15              Jan 18 2005
Smith           15              Jan 19 2005
```

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

Field	Description
Username	The user name.
Privilege	The user's privilege level.

Field	Description
Password Expiry date	The user's password expiration date.

aaa accounting commands

The **aaa accounting commands** Global Configuration mode command defines the list of protocols that are used for commands accounting. To restore the default commands accounting method list, use the **no** form of this command.

Syntax

aaa accounting commands *privilege-level* {**default** | list-name} method}

no aaa accounting commands {**default** | *list-name*}

Parameters

- *privilege-level* —Specifies the command privilege level the method list applies to.

  Select one of the following:

  - 1—Defines a commands accouting method list for level 1 commands.
  - 7—Defines a commands accouting method list for level 7 commands.
  - 15—Defines a commands accouting method list for level 15 commands.

- **default**—Uses the listed commands accounting methods that follow this argument as the default method list.
- *list-name* —Specifies a name for the list of commands accounting methods. (Length: 1–20 characters)
- *method* —Specifies the method used for commands accounting. Select the method from the following list:

Keyword	Description
none	Uses no commands accounting
tacas	Uses the list of all TACACS+ server for commands accounting.

Default Configuration

The **default** method list exists with none as the only method

Command Mode

Global Configuration mode

User Guidelines

Use the aaa accounting commands command to specify a method list used for accounting the commands that are configured on the devices. The list includes protocols to use for the commands accounting.

The accounting list is applied to Exec mode, Privilege Exec mode and also configuration mode commands according to the level defined in the list.

In order to activate a method list it needs to be applied to a management interface (console, SSH or telnet) using the accounting commands line configuration mode command.

The none method can be only as a single method. The none method disables the commands acccounting.

Use the no form of the command to return the default method list to its default, or to delete a named method list.

Example

The following example configures a named commands accounting method list for level 15 commands. The accounting information is sent to the list of TACACS+ servers.

```
switchxxxxxx(config)# aaa accounting commands 15 act_comm15 tacacs
```

accounting commands

-

show accounting methods

Use the show accounting methods Privileged EXEC mode command to display the Command Accounting methods and the management interfaces to which they were applied.

Syntax

show accounting methods

Parameters

N/A

Defaults

N/A

Example

Example 1

```
switchxxxxxx#show accounting methods
commands level 1 Accounting Method Lists
----------------------------------------
L1Acc : Tacacs
default : None
commands level 7 Accounting Method Lists
----------------------------------------
```

```
default : Tacacs
commands level 15 Accounting Method Lists
-----------------------------------------
default : None
Line Command Level 1 Command Level 7 Command Level 15
Method List Method List Method List
------- -------------------- -------------------- --------------------
Console default default default
Telnet default default default
SSH L1Acc default default
```

passwords complexity keyboard-pattern

Use the passwords complexity keyboard-pattern Global Configuration mode command to enable QWERTY keyboard pattern related restriction as part of password complexity settings.

Use the no form of the command to disable the QWERTY keyboard pattern related restriction.

Syntax

passwords complexity keyboard-pattern

no passwords complexity keyboard-pattern

Parameters

N/A

Default Configuration

Keyboard-pattern Password complexity setting is Disabled by default.

Command Mode

Global Configuration mode

User Guidelines

Use the **passwords complexity keyboard-pattern** command to define that a password cannot contain more than 3 consecutive characters on a QWERTY keyboard. The restriction applies only to letters and numbers on the keyboard and not to symbols. Both forward and reverse character sequences are prohibited.

The restriction is applied to the password defined using one of the following command:

- username
- enable password
- password

Example

The following example enables the key-board-pattern based password restriction.

```
switchxxxxxx(config)# passwords complexity keyboard-pattern
```

aaa accounting login start-stop

Use the **aaa accounting login start-stop** 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.

Name	Start Message	Stop Message	Description
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 radius
```

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

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 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	The arbitrary value that 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	Indicates 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
```

aaa accounting update periodic

To enable sending periodic interim accounting updates and to set the interval between the updates, use the aaa accounting update periodic Global Configuration mode command. Use the no form of this command to disable accounting periodic updates.

Syntax

aaa accounting update periodic *minutes*

no aaa accounting update periodic

Parameters

- *minutes* - The interval, in minutes, between the periodic accounting updates (Range: 1-65535 minutes)

Default Configuration

Periodic updates are disabled

Command Mode

Global Configuration mode

User Guidelines

If accounting periodic updates are enabled an accounting Interim-Update packet will be sent periodically for each 802.1x or login session, in an interval defined in this command.

If the Access-Accept sent by the RADIUS server includes the Acct-Interim-Interval attribute (type 85), then the actual interval between updates will be set to the larger value between the interval configured in this command and the value that is included in the attribute.

Example

In the following example, periodic accounting updates are enabled and the interval between the updates is set to 5 minutes:

```
switchxxxxxx(config)# aaa accounting update periodic 5
```

show accounting

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

Syntax

show accounting

Command Mode

User EXEC mode

Example

The following example displays information about the accounting status.

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

passwords complexity

Use the **passwords complexity** Global Configuration mode commands to control the minimum requirements from a password when password complexity is enabled. Use the **no** form of these commands to return to default.

Syntax

passwords complexity {**min-length** number} | {**min-classes** number} | {**no-repeat** number} | **not-current** | **not-username** | **not-manufacturer-name**

no passwords complexity min-length | **min-classes** | **no-repeat** | **not-current** | **not-username** | **not-manufacturer-name**

Parameters

- **min-length** number—Sets the minimal length of the password. (Range: 8–64)
- **min-classes** number—Sets the minimal character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard). (Range: 1–4)
- **no-repeat** number—Specifies the maximum number of characters in the new password that can be repeated consecutively. (Range: 1–16)
- **not-current**—Specifies that the new password cannot be the same as the current password.
- **not-username**—Specifies that the password cannot repeat or reverse the user name or any variant reached by changing the case of the characters.
- **not-manufacturer-name**—Specifies that the password cannot repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

Default Configuration

The minimal length is 8.

The number of classes is 3.

The default for no-repeat is 3.

All the other controls are enabled by default.

Command Mode

Global Configuration mode

Example

The following example configures the minimal required password length to 10 characters.

```
switchxxxxxx(config)# passwords complexity min-length 10
```

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

Password aging is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

The password aging setting is relevant to local database users, enable passwords and line passwords.

If password aging is enabled, when a user logs into the device within the 10 days preceding the password expiration date, a warning will be displayed alerting the user that the password will expire soon. The user is granted access to the device without changing the password. At this stage it is the user's responsibility to change the password before the expiration date.

Is the user logs into the device after the password expiration date, they are prompted to enter a new password and are not allowed access to the device management until a new password has been configured.

To disable password aging, use **passwords aging 0**.

Example

The following example configures the aging time to be 24 days.

```
witchxxxxxx(config)# passwords aging 24
```

password complexity history

The passwords complexity 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 return to the default setting

Syntax

passwords complexity history *number*

no passwords complexity history

Parameters

number—Specifies the number of password changes required before a password can be reused. (Range: 3–12).

Default Configuration

By default the number of passwords changes that are needed before password reuse is 12.

Command Mode

Global configuration mode.

User Guidelines

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

The local user history is maintained for users up to the number of local users supported on the device.

Password history is not checked during a configuration download.

The password history is kept even if the password history check is disabled.

Example

The following example sets the number of password changes required before a password can be reused to 10.

```
switchxxxxxx(config)# passwords complexity history 10
```

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

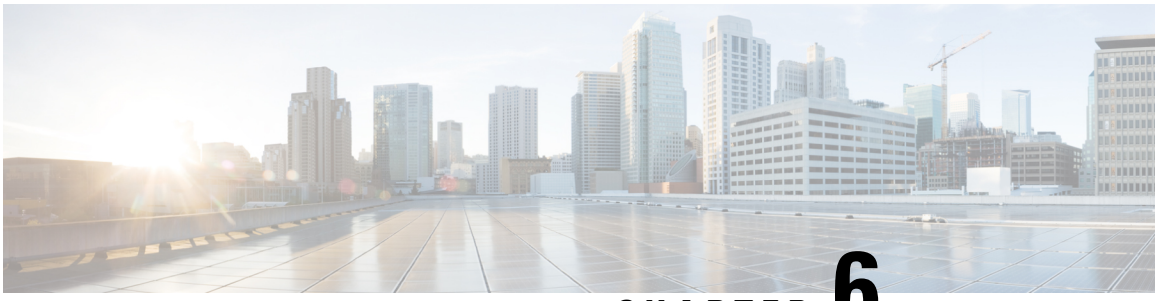
N/A

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords history is enabled, the number of previous passwords to check is 12
Passwords complexity is enabled with the following attributes:
 Minimal length: 8 characters
 Minimal classes: 3
 Maximum consecutive same characters: 3
 Password cannot include more than 2 sequential numbers or characters
Password cannot contain the username, manufacturer name or product name
Password must be different from current password
Password cannot contain commonly used passwords or known breached passwords
```



CHAPTER 6

Auto-Update and Auto-Configuration

This chapter contains the following sections:

- boot host auto-config, on page 161
- boot host auto-update, on page 162
- show boot, on page 163
- ip dhcp tftp-server ip address, on page 164
- ip dhcp tftp-server file, on page 165
- ip dhcp tftp-server image file, on page 165
- show ip dhcp tftp-server, on page 166

boot host auto-config

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

Syntax

boot host auto-config [**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: 1-16 characters)

Default Configuration

Enabled by default with the **auto** option.

Command Mode

Global Configuration mode

User Guidelines

The TFTP or SCP protocol is used to download/upload a configuration file.

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

```
switchxxxxxx(config)# 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.

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

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

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

boot host auto-update

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

Syntax

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

no boot host auto-update

Parameters

- **tftp**—Only the TFTP protocol is used by auto-update.
- **scp**—Only the SCP protocol is used by auto-update.
- **auto** (Default)—Auto-update uses the TFTP or SCP protocol depending on the Indirect image 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: 1-16 characters)

Default Configuration

Enabled by default with the **auto** option.

Command Mode

Global Configuration mode

User Guidelines

The TFTP or SCP protocol is used to download/upload an image file.

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

```
switchxxxxxx(config)# boot host auto-update auto scon
```

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

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

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

```
switchxxxxxx(config)# boot host auto-update scp
```

show boot

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

Syntax

show boot

Command Mode

Privileged EXEC mode

Examples

```
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: auto
SCP protocol will be used for files with extension: scp
Configuration file auto-save: enabled
Auto Config State: Finished successfully
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: enabled
Download Protocol: scp
Configuration file auto-save: enabled
Auto Config State: Opening <hostname>-config file
      Auto Update
      -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
"Download Protocol: scp
Configuration file auto-save: enabled
Auto Config State: Downloading configuration file
      Auto Update
```

```
      -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: tftp
Configuration file auto-save: enabled
Auto Config State: Searching device hostname in indirect file
      Auto Update
      -----------
Image Download via DHCP: enabled
switchxxxxxx# show boot
Auto Config
------------
Config Download via DHCP: enabled
Download Protocol: tftp
Configuration file auto-save: enabled
      Auto Update
      -----------
Image Download via DHCP: enabled
Auto Update State: Downloaded indirect image file
Indirect Image filename: /image/indirectimage.txt
```

ip dhcp tftp-server ip address

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

Default Configuration

No IP address

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Examples

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

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

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

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

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

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

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 from the backup server when it has not been received from the DHCP server. 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

User Guidelines

The backup server can be a TFTP server or an SCP server.

Examples

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

ip dhcp tftp-server image file

Use the **ip dhcp tftp-server image file** Global Configuration mode command to set the indirect file name of the image file to be downloaded from the backup server when it has not been received from the DHCP server. Use the **no** form of this command to remove the file name.

Syntax

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

no ip dhcp tftp-server image file

Parameters

- ***file-path***—Full indirect file path and name of the configuration file on the server.

Default Configuration

No file name

Command Mode

Global Configuration mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Examples

```
switchxxxxxx(config)# ip dhcp tftp-server image file imag/imag-file
```

show ip dhcp tftp-server

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

Syntax

show ip dhcp tftp-server

Command Mode

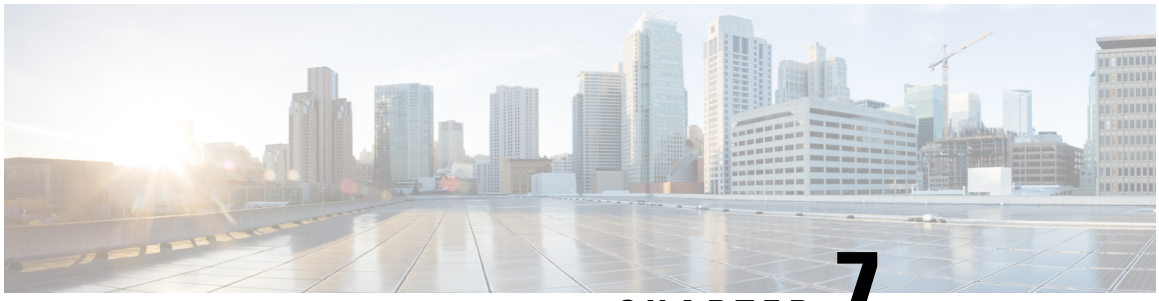
User EXEC mode

User Guidelines

The backup server can be a TFTP server or a SCP server.

Example

```
show ip dhcp tftp-server
server address
active 1.1.1.1 from sname
manual 2.2.2.2
file path on server
active conf/conf-file from option 67
manual conf/conf-file1
```



CHAPTER 7

Bluetooth Commands

This chapter contains the following sections:

- bluetooth device-name, on page 167
- bluetooth pin, on page 168
- show bluetooth status, on page 168
- shutdown, on page 170

bluetooth device-name

Use the bluetooth device-name command in Bluetooth Interface mode to configure the Bluetooth device name to use in the pairing process, and in subsequent Bluetooth operations. Use the no form of command to return to the default setting.

Syntax

bluetooth device-name *device-name*

no bluetooth device-name

Parameters

device name- Specifies a name associated with the Bluetooth interface. (Length: 1–20 characters).

Default Configuration

The default device-name is the device hostname.

Command Mode

Bluetooth interface Configuration mode.

User Guidelines

Use the bluetooth device-name command to configure the device-name associated with the Bluetooth interface. The Bluetooth device-name is used to identify the Bluetooth interface in the Bluetooth pairing process. If a Bluetooth device-name is not configured then the device hostname will be used as the device-name.

Examples

The following example shows how enter the Bluetooth interface configuration mode and configuring "Switch BT" as the Bluetooth interface device-name:

```
switchxxxxxx(config)# interface bluetooth 0
switchxxxxxx(config-if)# bluetooth device-name "Switch BT"
```

bluetooth pin

Use the bluetooth pin command in Bluetooth Interface mode to configure the 6-digit pin used in the pairing process. Use the no form of command to return to the default setting.

Syntax

bluetooth pin *pin*

no bluetooth pin.

Parameters

pin- a 4-digit personal identification number

Default Configuration

The default PIN is 9999.

Command Mode

Bluetooth interface Configuration mode.

User Guidelines

Use the bluetooth pin command to configure the 4-digit PIN which is used use in the Bluetooth pairing process between the device Bluetooth interface and a Bluetooth partner.

Examples

This example shows how to configure a pin of 1234 on the Bluetooth interface:

```
switchxxxxxx(config)# interface bluetooth 0
 switchxxxxxx(config-if)# shutdown
```

show bluetooth status

To display information about the Bluetooth interface configuration and status, use the show bluetooth status command in Privileged EXEC mode.

Syntax

show bluetooth status

Default Configuration

N/A

Command Mode

Privileged EXEC mode.

User Guidelines

Use the show bluetooth status command, to display information about the device bluetooth interface.

Examples

Example 1

This example shows BT interface information at the default state when dongle is not inserted into USB port:

```
switchxxxxxx# show bluetooth status
Dongle MAC: Not Available
BT Dongle Present: no
State: not ready
BT Local Name: switch112233 (the default)
PIN: 999999 (the default)
BT Partner Name: Not Available
```

Example 2

The following example displays the Bluetooth interface information when a dongle is inserted into USB port, and the user configured on the Bluetooth interface a Device Name and PIN. The Bluetooth interface is discoverable but did not connect yet with a remote Bluetooth partner:

```
switchxxxxxx# show bluetooth status
Dongle MAC: 00:1a:7d:da:71:13
Bus: USB
BT Dongle Present: Yes
State: Discoverable
BT Local Name: My_BT
PIN (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
BT Partner Name: Not Available
```

Example 3

The following example displays the Bluetooth interface information when it is paired and connected to a remote Bluetooth partner:

```
switchxxxxxx# show bluetooth status
Dongle MAC: 00:1a:7d:da:71:13
Bus: USB
BT Dongle Present: Yes
State: Connected
BT Local Name: My_BT
PIN (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
BT Partner Name: Tablet123
```

Example 4

The following example displays the Bluetooth interface information when it is paired and connected to a remote Bluetooth partner:switchxxxxxx# show bluetooth status

```
switchxxxxxx# show bluetooth status
Dongle MAC: 00:1a:7d:da:71:13
Bus: USB
```

```
BT Dongle Present: Yes
State: Admin Down
BT Local Name: My_BT
PIN (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
BT Partner Name: Not available
```

shutdown

Use the shutdown command in Interface (Bluetooth) Configuration mode to disable the operation of the Bluetooth interface. Use the no form of command to return to the default setting.

Syntax

shutdown

no shutdown

Default Configuration

he Bluetooth interface is active by default

Command Mode

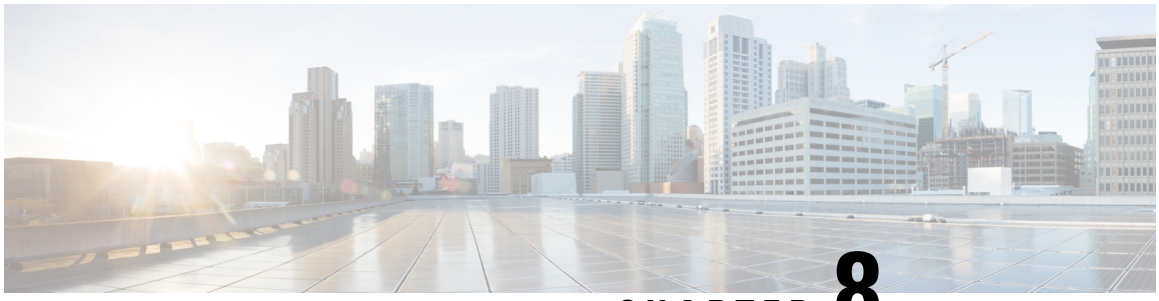
Interface (Bluetooth) Configuration mode.

Examples

Example 1

The following example shuts down the Bluetooth operation.

```
switchxxxxxx(config)# interface bluetooth 0
 switchxxxxxx(config-if)# shutdown
```



CHAPTER 8

Bonjour Commands

This chapter contains the following sections:

- bonjour enable, on page 171
- bonjour interface range, on page 171
- show bonjour, on page 172

bonjour enable

To enable Bonjour globally, use the **bonjour enable** command in Global Configuration mode. To disable Bonjour globally, use the **no** format of the command.

Syntax

bonjour enable

no bonjour enable.

Default Configuration

Enable

Command Mode

Global Configuration mode

Examples

```
switchxxxxxx(config)# bonjour enable
```

bonjour interface range

To add L2 interfaces to the Bonjour L2 interface list, use the **bonjour interface range** command in Global Configuration mode. To remove L2 interfaces from this list, use the **no** format of the command.

Syntax

bonjour interface range *interface-list*

no bonjour interface range [*interface-list*]

Parameters

- ***interface-list***—Specifies a list of interfaces. Only interfaces supporting L2 Multicast forwarding can be specified. The follow: LAN and point, which support be of the following types: OOB, Ethernet port, Port-channel, and VLAN.

Default Configuration

The list includes the Default VLAN and OOB.

Command Mode

Global Configuration mode

User Guidelines

The Bonjour L2 interface list specifies a set of interfaces on which Bonjour is enabled.

Use the **bonjour interface range** *interface-list* command, to add the specified interfaces to the Bonjour L2 interface list.

Use the **no bonjour interface range** *interface-list* command, to remove the specified interfaces from the Bonjour L2 interface list.

Use the **no bonjour interface range** command, to clear the Bonjour L2 interface list.

Examples

```
switchxxxxxx(config)# bonjour interface range VLAN 100-103
```

show bonjour

To display Bonjour information, use the **show bonjour** command in Privileged EXEC mode.

Syntax

show bonjour [*interface-id*]

Parameters

- ***interface-id***—Specifies an interface.

Command Mode

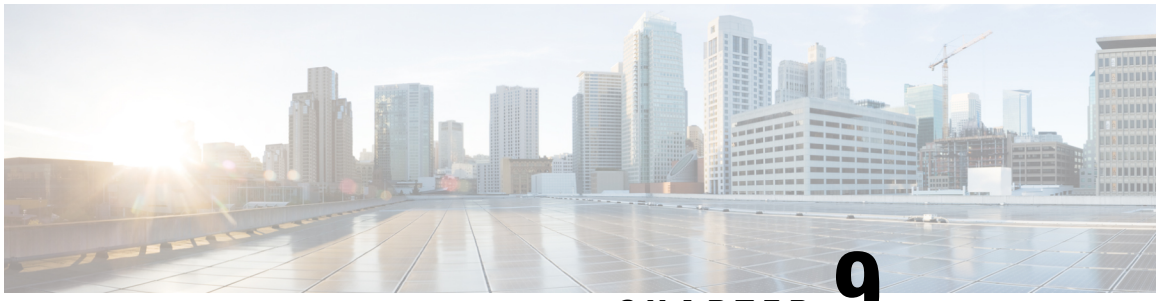
Privileged EXEC mode

Examples

The example displays Bonjour status.

```
switchxxxxxx# show bonjour
Bonjour global status: enabled
```

```
Bonjour L2 interfaces list: vlans 1
Service     Admin Status     Oper Status
-------     ------------     --------------
csco-sb     enabled              enabled
http        enabled              enabled
https       enabled              disabled
ssh         enabled              disabled
telnet      enabled              disabled
```



CHAPTER 9

CA Certificate Commands

This chapter contains the following sections:

- ca-certificate install, on page 175
- ca-certificate revoke, on page 176
- show ca-certificate, on page 177
- show ca-certificate revocation, on page 179

ca-certificate install

To manually install a CA certificate, use the **ca-certificate install** command in Global Configuration mode. To remove a static CA certificate, use the **no** form of this command.

Syntax

ca-certificate install name *name* [**owner** owner]

no ca-certificate install {**name** *name* | **owner** *owner*}

Parameters

- ***name***—Specifies the certificate name. The range is from 1 to 160 characters.
- ***owner***—specifies the owner of the certificate. This is a string of 0 to 32 characters. If an owner is not specified, the default owner is "Static".

When adding a certificate, the certificate itself should follow the command on the command line.

Default Configuration

There are no installed certificates.

Command Mode

Global Configuration mode

User Guidelines

Use the **ca-certificate install** *name* command to install a CA certificate.

Following the command, the user will be prompted to enter the certificate in the command line.

The user will need to enter or paste the certificate. Entering a period on a separate line indicates that the certificate input is complete.

The entered certificate must use the pem format.

A certificate will not be valid if the system clock was not set by user or synchronized with SNTP, or based on hardware based Real Time Clock (RTC).

Up to 256 certificates can be installed.

When using the **no** form of the command to remove certificates, a specific certificate can be removed by **name**. Alternatively, the **owner** keyword can be used to remove all static certificates belonging to a specific owner.

Example 1. The following example installs a CA certificate from the command line:

```
switchxxxxxx(config)# ca-certificate install root1
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-----
switchxxxxxx(config)#
```

ca-certificate revoke

To add a certificate to the revocation list, use the **ca-certificate revoke** command in Global Configuration mode. To remove a certificate from the revocation list, use the **no** form of this command.

Syntax

ca-certificate revoke issuer *issuer* **serial-number** *serial-number*

no ca-certificate revoke issuer *issuer* **serial-number** *serial-number*

Parameters

- ***issuer***—The issuer string as it appears in the revoked certificate - including all parameters (Range: 1-160 characters).
- ***serial-number***—The serial number of the revoked certificate. This is a string in hexadecimal format (Range: 1-16 pairs of characters).

Default Configuration

There are no revoked certificates.

Command Mode

Global Configuration mode

User Guidelines

Use the **ca-certificate revoke** command to add a certificate to the revocation list.

When entering the issuer information, the full issuer string should be entered as it appears in the certificate. If the string contains spaces, it must be contained in quotation marks.

Adding a certificate to this list will change the status of this certificate to "revoked" if it is installed. If the certificate is not installed, it will receive the revoked status if it is installed at a later date.

Up to 512 certificates can be added to the revocation list.

Example 1. The following example adds a CA certificate to the revocation list:

```
switchxxxxxx(config)# ca-certificate revoke issuer "C=US, O=GlobalSign nv-sa, CN=GlobalSign
 Organization Validation" serial-number 10ad0044a8418ad5005e45b6
switchxxxxxx(config)#
```

show ca-certificate

To display the CA certificates installed on the device and their status, use the **show ca-certificate** command in Privileged EXEC mode.

Syntax

show ca-certificate [name *name*][type *type*][owner *owner-name*][detailed]

Parameters

- **name** *name* - Specifies the certificate name. (Range: 1-160 characters).
- **type** *type*—Specifies the certificate type. The possible values are static, dynamic or signer.
- **owner** *owner-name*—Specifies the name of the certificate owner - this is the application that installed a dynamic certificate. (Range: 1-32 characters).
- **detailed** - This optional parameter shows detailed information of the displayed certificates. If this parameter is not used, only limited information will be displayed for each certificate.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show ca-certificate** command to display all installed CA certificates.

Use the optional **name, type** and **owner** parameters to display the information of a subset of certificates.

Example 1 The following example displays brief information for all static CA certificates.

```
switchxxxxxx# show ca-certificate type static
Name           Type    Owner     Valid From   Valid To     Status
-------------  ------  --------  -----------  -----------  ----------
local.cert     static  rnd       03-Aug-2019  03-Aug-2020  Valid
app1.cert1     static  app1      16-Jan-2021  16-Jul-2023  Premature
app1.cert2     static  app1      15-Mar-2017  14-Mar-2018  Expired
trusted-cert1  static  app2      27-Jun-2019  26-Jun-2024  Valid
certif3        static  app3      08-Feb-2018  08-Feb-2020  Revoked
```

Example 2 The following example displays detailed information for all CA certificates:

```
switchxxxxxx# show ca-certificate detailed
>C-CountryName, ST-StateOrProvinceName, L-Locality, O-Organization,
>OU-OrganizationalUnit, CN-CommonName
cert1
  Type: Signer
  Owner: N/A
  Version: 3 (0x2)
  Serial Number: 10:ad:00:44:a8:41:8a:d5:00:5e:45:b6
  Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Status: Valid
  Validity
    Not Before: Nov 21 08:00:00 2015 GMT
    Not After : Nov 22 07:59:59 2020 GMT
  Subject: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Public Key Type: ECDSA_P256
  Public Key Length: 2048 bits
    Signature Algorithm: sha256RSA
 certA
  Type: Static
  Owner: Static
  Parent: cert1
  Version: 3 (0x2)
  Serial Number: 10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
  Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Status: Not Valid (expired)
  Validity
    Not Before: Nov 21 08:00:00 2016 GMT
    Not After : Nov 22 07:59:59 2017 GMT
  Subject: C=US, ST=California, L=San Francisco, O=AKB Foundation, Inc.,
           CN=*.wikipedia.org
  Finger print: DC72343 DC88A988 127897BC BB789788
  Public Key Type: ECDSA_P256
  Public Key Length: 2048 bits
    Signature Algorithm: sha256RSA
  certB
  Type: Dynamic
  Owner: PnP
  Parent: cert1
  Version: 3 (0x2)
  Serial Number: 88:cc:55:ae:a8:41:8a:d5:00:5e:45:b6
  Issuer: C=US, O=Google Trust Services, CN=GTS CA 101
  Status: Not Valid (revoked)
  Validity
    Not Before: Sep 21 08:00:00 2019 GMT
    Not After : Sep 22 07:59:59 2020 GMT
  Subject: C=US, S=California, L=Mountain View O=Google LLC, CN=*.google.com
  Finger print: DC789788 DC88A988 127897BC BB789788
  Public Key Type: ECDSA_P256
  Public Key Length: 2048 bits
  Signature Algorithm: sha256RSA
```

show ca-certificate revocation

To display the CA certificate revocation list, use the **show ca-certificate revocation** command in Privileged EXEC mode.

Syntax

show ca-certificate revocation

Command Mode

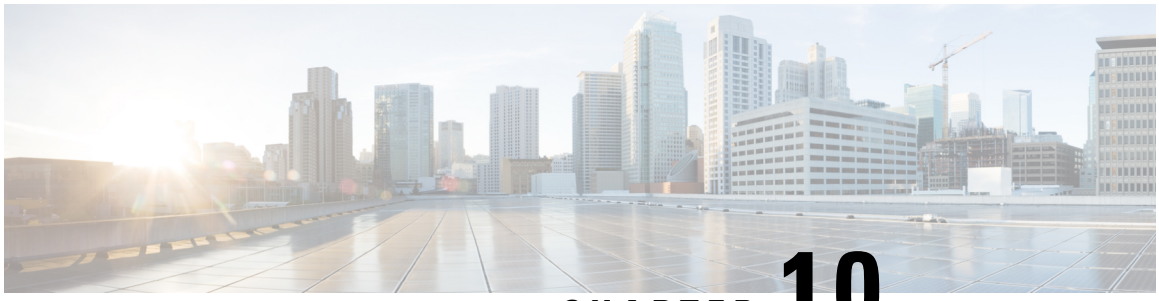
Privileged EXEC mode

User Guidelines

Use the **show ca-certificate revocation** command to display the CA certificate revocation list.

Example. The following displays the revocation list:

```
switchxxxxxx# show ca-certificate revocation
>C-CountryName, ST-StateOrProvinceName, L-Locality, O-Organization,
>OU-OrganizationalUnit, CN-CommonName
  Issuer: C=US, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation
  Serial Number: 10:ad:00:44:a8:41:8a:d5:00:5e:45:b6
-------------------------------------------------------------------------
  Issuer: C=US, O=Google Trust Services, CN=GTS CA 101
  Serial Number: 00:9e:44:1b:49:08:8d:75:bb:02:00:00:00:00:40:a5:b4
```



CHAPTER 10

CBD Probe Commands

This chapter contains the following sections:

- cbd probe enable, on page 181
- cbd address, on page 182
- cbd key, on page 183
- cbd connection enable, on page 183
- cbd reset, on page 184
- clear cbd probe database, on page 185
- show cbd , on page 186

cbd probe enable

To enable the Cisco Business Dashboard Probe operation on device, use the **cbd probe enable** command in Global Configuration mode. To disable the Cisco Business Dashboard Probe operation, use the **no** form of this command.

Syntax

cbd probe enable

no cbd probe enable

Default Configuration

Cisco Business Dashboard Probe is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the command to enable the Cisco Business Dashboard Probe on the device.

Example

The following example enables the Cisco Business Dashboard Probe on the device:

```
switchxxxxxx(config)# cbd probe enable
This operation may take a few seconds....
```

cbd address

To configure the details of the Cisco Business Dashboard, use the **cbd address** command in Global Configuration mode. To remove the details of the Cisco Business Dashboard, use the **no** form of this command.

Syntax

cbd address {*ip-address* | *hostname*} [**port** *port*]

no cbd address

Parameters

- **address** *ip-address*—Specifies the Cisco Business Dashboard IP address. This can be an IPv4 address.
- **address** *hostname* — Specifies the Cisco Business Dashboard as a hostname (Range: 1–158 characters. Maximum label size of each part of the host name: 63).
- **port** — Specifies the TCP port used to connect to Cisco Business Dashboard. (Range: 1-65535)

Default Configuration

No address is configured. CBD **port** default is 443.

Command Mode

Global Configuration mode

User Guidelines

Use the **cbd address** command to configure the Cisco Business Dashboard IP address and the TCP port to use to connect to the Cisco Business Dashboard. The **cbd connection enable** configuration must be removed prior to making changes to this parameter.

Examples

The following example configures the IPv4 address of the Cisco Business Dashboard to 1.1.1.1 and sets the TCP port to 8443.

```
switchxxxxxx(config)# cbd address 1.1.1.1 port 8443
```

In the following example configuration of the Cisco Business Dashboard IPv4 address fails because connection to Dashboard is enabled.

```
switchxxxxxx(config)# cbd address 1.1.1.1
Command failed!
Please disable connection to Cisco Business Dashboard before configuring this command, using
 command "no cbd connection enable". Only after configuring all Dashboard settings (Dashboard
 address, Key parameters, Organization and Network name) re-enable connection (command "cbd
 connection enable") to allow Probe connection to Cisco Business Dashboard
```

cbd key

To configure the key ID and secret of the Cisco Business Dashboard, use the **cbd key** command in Global Configuration mode. To remove Cisco Business Dashboard key ID and secret configuration, use the **no** form of this command.

Syntax

cbd key id *id-string* **secret** *secret-string*

encrypted cbd key id *id-string* **secret** *encrypted-secret-string*

no cbd key

Parameters

- **id** *id-string*—Specifies the key ID to use for initial authentication between the Cisco Business Dashboard Probe running on the device and the Cisco Business Dashboard (A string of 24 hexadecimal digits).
- **secret** *secret-string*— Specifies the secret to use for authentication, can be specified as an alphanumeric string **without** white-spaces. The key can be up to 160 characters.
- **secret** *encrypted-secret-string* — Same as the *secret-string* parameter, but the secret is in encrypted form.

Default Configuration

CBD key ID and secret are not defined.

Command Mode

Global Configuration mode

User Guidelines

Use the **cbd key** command to configure the Cisco Business Dashboard key ID and secret. The **cbd connection enable** configuration must be removed prior to making changes to this parameter.

Example

The following example configures the key ID and secret of the Cisco Business Dashboard used for initial authentication:

```
switchxxxxxx(config)# cbd key id 5cecde9f21bb450005fb790b secret secretExample123
```

cbd connection enable

To configure the probe to connect with Cisco Business Dashboard, use the **cbd connection enable** command in Global Configuration mode. To disable probe connection to the Cisco Business Dashboard, use the **no** form of this command.

Syntax

cbd connection enable

no cbd connection enable

Default Configuration

Probe is not enabled for connection to Cisco Business Dashboard.

Command Mode

Global Configuration mode

User Guidelines

Use the **cbd connection enable** command to enable the probe to connect to the Cisco Business Dashboard. The configuration of this command will trigger the Cisco Business Dashboard Probe to connect to the Cisco Business Dashboard if the CBD Probe is enabled.

The **cbd organization name**, **cbd network name**, **cbd address** and **cbd key** settings must be configured for the **cbd connection enable** command to succeed. Use the **no cbd connection enable** to disconnect the Probe from the Cisco Business Dashboard and to allow the user to change the Cisco Business Dashboard settings mentioned above.

Examples

The following example enables the probe to connect to the Cisco Business Dashboard:

```
switchxxxxxx(config)# cbd connection enable
```

In the following example the command fails because some of the Dashboard settings needed for connection were not configured:

```
switchxxxxxx(config)# cbd connection enable
Command failed. Please make sure all of the following dashboard parameters are configured:
 dashboard address, organization name, network name and key;
```

cbd reset

To reset Cisco Business Dashboard Probe connection to the Cisco Business Dashboard use the **cbd reset** command in Privileged EXEC mode.

Syntax

cbd reset

Command Mode

Privileged EXEC mode

User Guidelines

Use the **cbd reset** command to reset the connection to the Cisco Business Dashboard. Applying the command will disconnect current connection with Dashboard, flush CBD probe cached data and then attempt to reconnect to the Cisco Business Dashboard.

The command will be executed only if the Probe Agent is enabled (command cbd probe enable, on page 181) and connection to Cisco Business Dashboard is also enabled (command cbd connection enable, on page 183).

Examples

The following example executes an attempt to reconnect using the configured key ID and secret:

```
switchxxxxxx# cbd reset
```

In the following example the reset command fails because Probe connection to Network Cisco Business Dashboard is not enabled:

```
switchxxxxxx# cbd reset
Operation failed because Probe connection to Cisco Business Dashboard is not enabled.
Please enable conntection to Cisco Business Dashboard using command "cbd connection enable".
```

In the following example the reset command fails because Probe agent is not enabled on device:

```
switchxxxxxx# cbd reset
Operation failed because Probe is not enabled
Please enable Probe using command "cbd probe enable".
```

clear cbd probe database

To clear the Cisco Business Dashboard Probe database use the **clear cbd probe database** command in Privileged EXEC mode.

Syntax

clear cbd probe database

Command Mode

Privileged EXEC mode

User Guidelines

Use the **clear cbd probe database** to clear the Cisco Business Dashboard Probe database.

The command will be executed only if the Cisco Business Dashboard Probe Agent is disabled.

Examples

The following example clears the Cisco Business Dashboard Probe Database:

```
switchxxxxxx# clear cbd probe database
```

In the following example, the clear command fails because the Cisco Business Dashboard Probe is enabled on the switch:

```
switchxxxxxx# clear cbd probe database
Operation failed because Cisco Business Dashboard Probe is enabled on the switch.
Please disable Probe on switch using command "no cbd probe enable".
```

show cbd

To display information about Cisco Business Dashboard Probe Configuration and status, use the **show cbd** command in Privileged EXEC mode.

Syntax

show cbd

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show cbd** command, to display information about the Cisco Business Dashboard Probe running on the device.

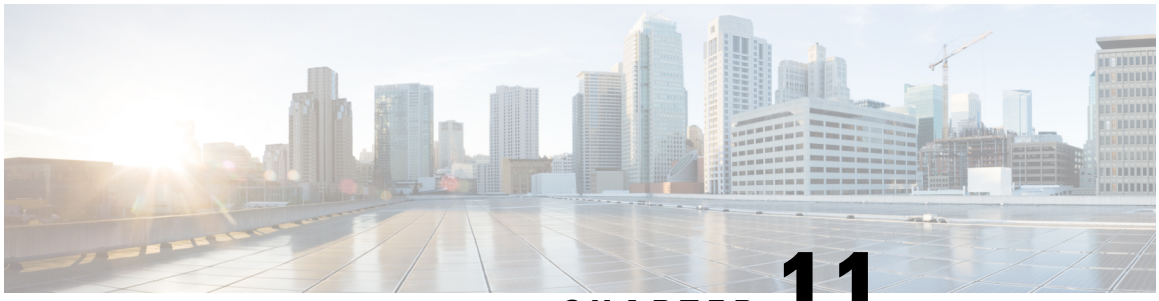
Example

The following example shows the output from the **show cbd** command:

```
switchxxxxxx# show cbd
Network Probe is enabled
Operational status: Active
Probe version: 1.1.2.20181019
Dashboard address: 1.1.1.1
Dashboard port: 443
Key ID: MyKey
Key Secret (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
Organization name: ABC Company
Network name: my network
Dashboard status: connected
```

The following table describes the different Cisco Business Dashboard Probe setting and behavior and the relevant Administrative & Operational state display.

Cisco Business Dashboard Probe Setting and Status	Administrative State indication	Operational State indication
Cisco Business Dashboard Probe Disabled	Disabled	Inactive
Cisco Business Dashboard Probe Enabled and active	Enabled	Active
Cisco Business Dashboard Probe Enabled but is not active (indicates a failure)	Enabled	Fault



CHAPTER 11

CDP Commands

This chapter contains the following sections:

- cdp advertise-v2, on page 187
- cdp appliance-tlv enable, on page 188
- cdp device-id format, on page 189
- cdp enable, on page 189
- cdp holdtime, on page 190
- cdp log mismatch duplex, on page 190
- cdp log mismatch native, on page 191
- cdp log mismatch voip, on page 191
- cdp mandatory-tlvs validation, on page 192
- cdp pdu, on page 193
- cdp run, on page 193
- cdp source-interface, on page 194
- cdp timer, on page 195
- clear cdp counters, on page 195
- clear cdp table, on page 196
- show cdp, on page 196
- show cdp entry, on page 197
- show cdp interface, on page 199
- show cdp neighbors, on page 199
- show cdp tlv, on page 203
- show cdp traffic, on page 205

cdp advertise-v2

To specify version 2 of transmitted CDP packets, use the **cdp advertise-v2** command in Global Configuration mode. To specify version 1, use the **no** form of this command.

Syntax

cdp advertise-v2

no cdp advertise-v2

Default Configuration

Version 2.

Command Mode

Global configuration mode

Example

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# cdp advertise-v2
```

cdp appliance-tlv enable

To enable sending of the Appliance TLV, use the **cdp appliance-tlv enable** command in Global Configuration mode. To disable the sending of the Appliance TLV, use the **no** form of this command.

Syntax

cdp appliance-tlv enable

no cdp appliance-tlv enable

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

This MIB specifies the Voice Vlan ID (VVID) to which this port belongs:

- **0**—The CDP packets transmitting through this port contain Appliance VLAN-ID TLV with value of 0. VoIP and related packets are expected to be sent and received with VLAN-ID=0 and an 802.1p priority.
- **1..4094**—The CDP packets transmitting through this port contain Appliance VLAN-ID TLV with N. VoIP and related packets are expected to be sent and received with VLAN-ID=N and an 802.1p priority.
- **4095**—The CDP packets transmitting through this port contain Appliance VLAN-ID TLV with value of 4095. VoIP and related packets are expected to be sent and received untagged without an 802.1p priority.
- **4096**—The CDP packets transmitting through this port do not include Appliance VLAN-ID TLV; or, if the VVID is not supported on the port, this MIB object will not be configurable and will return 4096.

Example

```
switchxxxxxx(config)# cdp appliance-tlv enable
```

cdp device-id format

To specify the format of the Device-ID TLV, use the **cdp device-id format** command in Global Configuration mode. To return to default, use the **no** form of this command.

Syntax

cdp device-id format {mac | serial-number | hostname}

no cdp device-id format

Parameters

- **mac**—Specifies that the Device-ID TLV contains the device's MAC address.
- **serial-number**—Specifies that Device-ID TLV contains the device's hardware serial number.
- **hostname**—Specifies that Device-ID TLV contains the device's hostname.

Default Configuration

MAC address is selected by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp device-id format serial-number
```

cdp enable

Tp enable CDP on interface, use the **cdp enable** command in Interface (Ethernet) Configuration mode. To disable CDP on an interface, use the **no** form of the CLI command.

Syntax

cdp enable

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

For CDP to be enabled on an interface, it must first be enabled globally using cdp advertise-v2, on page 187.

Example

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config-if)# interface gi1/0/1
switchxxxxxx(config-if)# cdp enable
```

cdp holdtime

To specify a value of the Time-to-Live field into sent CDP messages, use the **cdp holdtime** command in Global Configuration mode. To return to default, use the **no** form of this command.

Syntax

cdp holdtime *seconds*

no cdp holdtime

Parameters

seconds—Value of the Time-to-Live field in seconds. The value should be greater than the value of the Transmission Timer.

Parameters range

seconds—10 - 255.

Default Configuration

180 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp holdtime 100
```

cdp log mismatch duplex

To enable validating that the duplex status of a port received in a CDP packet matches the ports actual configuration and generation the SYSLOG duplex mismatch messages if they do not match, use the **cdp log mismatch duplex** command in Global Configuration mode and Interface (Ethernet) Configuration mode. To disable the generation of the SYSLOG messages, use the **no** form of the CLI command.

Syntax

cdp log mismatch duplex

no cdp log mismatch duplex

Default Configuration

The switch reports duplex mismatches from all ports.

Command Mode

Global Configuration mode

Interface (Ethernet) Configuration mode

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# cdp log mismatch duplex
```

cdp log mismatch native

To enable validating that the native VLAN received in a CDP packet matches the actual native VLAN of the port and generation the SYSLOG VLAN native mismatch messages if they do not match, use the **cdp log mismatch native** Global and Interface Configuration mode command in Global Configuration mode and Interface (Ethernet) Configuration mode. To disable the generation of the SYSLOG messages, use the **no** format of the CLI command.

Syntax

cdp log mismatch native

no cdp log mismatch native

Default Configuration

The switch reports native VLAN mismatches from all ports.

Command Mode

Global Configuration mode

Interface (Ethernet) Configuration mode

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# cdp log mismatch native
```

cdp log mismatch voip

To enable validating that the VoIP status of the port received in a CDP packet matches its actual configuration and generation the SYSLOG voip mismatch messages if they do not match, use the **cdp log mismatch voip** Global and Interface Configuration mode command in Global Configuration mode and Interface (Ethernet) Configuration mode. To disable the generation of the SYSLOG messages, use the **no** format of the CLI command.

Syntax

cdp log mismatch voip

no cdp log mismatch voip

Default Configuration

The switch reports VoIP mismatches from all ports.

Command Mode

Global Configuration mode

Interface (Ethernet) Configuration mode

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# cdp log mismatch voip
```

cdp mandatory-tlvs validation

To validate that all mandatory (according to the CDP protocol) TLVs are present in received CDP frames, use the **cdp mandatory-tlvs validation** command in Global Configuration mode. To disables the validation, use the **no** form of this command.

Syntax

cdp mandatory-tlvs validation

no cdp mandatory-tlvs validation

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

Use the command to delete CDP packets not including all the mandatory TLVs.

Example

This example turns off mandatory TLV validation:

```
switchxxxxxx(config)# no cdp mandatory-tlvs validation
```

cdp pdu

To specify CDP packets handling when CDP is globally disabled, use the **cdp pdu** command in Global Configuration mode. To return to default, use the **no** form of this command.

Syntax

cdp pdu [filtering | bridging | flooding]

no cdp pdu

Parameters

- **filtering**—Specify that when CDP is globally disabled, CDP packets are filtered (deleted).
- **bridging**—Specify that when CDP is globally disabled, CDP packets are bridged as regular data packets (forwarded based on VLAN).
- **flooding**—Specify that when CDP is globally disabled, CDP packets are flooded to all the ports in the product that are in STP forwarding state, ignoring the VLAN filtering rules.

Default Configuration

bridging

Command Mode

Global Configuration mode

User Guidelines

When CDP is globally enabled, CDP packets are filtered (discarded) on CDP-disabled ports.

In the flooding mode, VLAN filtering rules are not applied, but STP rules are applied. In case of MSTP, the CDP packets are classified to instance 0.

Example

```
switchxxxxxx(config)# cdp run
switchxxxxxx(config)# cdp pdu flooding
```

cdp run

To enable CDP globally, use the **cdp run** command in Global Configuration mode. To disable CDP globally, use the **no** form of this command.

Syntax

cdp run

no cdp run

Default Configuration

Enabled.

Command Mode

Global Configuration mode

User Guidelines

CDP is a link layer protocols for directly-connected CDP/LLDP-capable devices to advertise themselves and their capabilities. In deployments where the CDP/LLDP capable devices are not directly connected and are separated with CDP/LLDP incapable devices, the CDP/LLDP capable devices may be able to receive the advertisement from other device(s) only if the CDP/LLDP incapable devices flood the CDP/LLDP packets they receives. If the CDP/LLDP incapable devices perform VLAN-aware flooding, then CDP/LLDP capable devices can hear each other only if they are in the same VLAN. It should be noted that a CDP/LLDP capable device may receive advertisement from more than one device if the CDP/LLDP incapable devices flood the CDP/LLDP packets.

To learn and advertise CDP information, it must be globally enabled (it is so by default) and also enabled on interfaces (also by default).

Example

```
switchxxxxxx(config)# cdp run
```

cdp source-interface

To specify the CDP source port used for source IP address selection, use the **cdp source-interface** command in Global Configuration mode. To delete the source interface, use the **no** form of this command.

Syntax

cdp source-interface *interface-id*

no cdp source-interface

Parameters

interface-id—Source port used for Source IP address selection.

Default Configuration

No CDP source interface is specified.

Command Mode

Global Configuration mode

User Guidelines

Use the **cdp source-interface** command to specify an interface whose minimal IP address will be advertised in the TVL instead of the minimal IP address of the outgoing interface.

Example

```
switchxxxxxx(config)# cdp source-interface gi1/0/1
```

cdp timer

To specify how often CDP packets are transmitted, use the **cdp timer** command in Global Configuration mode. To return to default, use the **no** form of this command.

Syntax

cdp timer *seconds*

no cdp timer

Parameters

seconds—Value of the Transmission Timer in seconds. Range: 5-254 seconds.

Default Configuration

60 seconds.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# cdp timer 100
```

clear cdp counters

To reset the CDP traffic counters to 0, use the **clear cdp counters** command in Privileged EXEC mode.

Syntax

clear cdp counters [**global** | *interface-id*]

Parameters

- **global**—Clear only the global counters.
- ***interface-id***—Specifies the interface identifier of the counters that should be cleared.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command **clear cdp counters** without parameters to clear all the counters.

Use the **clear cdp counters global** to clear only the global counters.

Use the **clear cdp counters** *interface-id* command to clear the counters of the given interface.

Example

Example 1. The example clears all the CDP counters:

```
switchxxxxxx# clear cdp couters
```

Example 2. The example clears the CDP global counters.

```
switchxxxxxx# clear cdp couters global
```

Example 3. The example clears the CDP counters of Ethernet port gi1/0/1:

```
switchxxxxxx# clear cdp couters interface gi1/0/1
```

clear cdp table

To delete the CDP Cache tables, use the **clear cdp table** command in Privileged EXEC mode.

Syntax

clear cdp table

Command Mode

Privileged EXEC mode

Example The example deletes all entries from the CDP Cache tables:

```
switchxxxxxx# clear cdp table
```

show cdp

To display the interval between advertisements, the number of seconds the advertisements are valid and version of the advertisements, use the **show cdp** Privileged EXEC mode command in Privileged EXEC mode.

Syntax

show cdp

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show cdp
Global CDP information:
   cdp is globally enabled
   cdp log duplex mismatch is globally enabled
   cdp log voice VLAN mismatch is globally enabled
   cdp log native VLAN mismatch is globally disabled
```

```
Mandatory TLVs are
  Device-ID TLV (0x0001
  Address TLV (0x0002)
  Port-ID TLV (0x0003)
  Capabilities TLV (0x0004)
  Version TLV (0x0005)
  Platform TLV (0x0006)
Sending CDPv2 advertisements is enabled
Sending Appliance TLV is enabled
Device ID format is Serial Number
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
```

show cdp entry

To display information about specific neighbors, use the **show cdp entry** command in Privileged EXEC mode.

Syntax

show cdp entry {***** | *device-name}* [**protocol** | **version**]

Parameters

- *****—Specifies all neighbors
- **device-name**—Specifies the name of the neighbor.
- **protocol**—Limits the display to information about the protocols enabled on neighbors.
- **version**—Limits the display to information about the version of software running on the neighbors.

Default Configuration

All of the entry information is display if the protocol and version keywords are not specified.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show cdp entry
Device-ID: Site1-C1300-Stack-10
Advertisement version: 2
Platform: Cisco C1300-24P-4X (PID:C1300-24P-4X)-VSD
Capabilities: Router Switch IGMP
Interface: gi10, Port ID (outgoing port): gi2/0/20
Holdtime: 129
Version: 4.1.0.68
Duplex: full
Native VLAN: 1
Application: VoIP using VLAN 114
SysName: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
```

```
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 protocol
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 version
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Version: 4.0.0.81
Site1-C1200-8T-16#


switchxxxxxx# show cdp entry device.cisco.com version
Device-ID: Site1-C1300-Stack-10
Advertisement version: 2
Platform: Cisco C1300-24P-4X (PID:C1300-24P-4X)-VSD
Capabilities: Router Switch IGMP
Interface: gi10, Port ID (outgoing port): gi2/0/20
Holdtime: 129
Version: 4.1.0.68
Duplex: full
Native VLAN: 1
Application: VoIP using VLAN 114
SysName: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 protocol
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 version
-------------------------------------------
Device-ID: Site1-C1300-Stack-10
Version: 4.0.0.81
Site1-C1200-8T-16#


switchxxxxxx# show cdp entry device.cisco.com protocol
Device-ID: Site1-C1300-Stack-10
Addresses:
          IP 172.16.1.31
          IPv6 fe80::e64e:2dff:fe4a:32eb (link-local)
Site1-C1200-8T-16#
Site1-C1200-8T-16#
Site1-C1200-8T-16#sh cdp entry Site1-C1300-Stack-10 version


switchxxxxxx# show cdp entry device.cisco.com version
Device-ID: Site1-C1300-Stack-10
Version: 4.0.0.81
Site1-C1200-8T-16#
```

show cdp interface

To display information about ports on which CDP is enabled, use the **show cdp interface** command in Privileged EXEC mode.

Syntax

show cdp interface ***interface-id***

Parameters

interface-id—Port ID.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show cdp interface gi1/0/1
CDP is globally enabled
CDP log duplex mismatch
  Globally is enabled
  Per interface is enabled
CDP log voice VLAN mismatch
  Globally is enabled
  Per interface is enabled
CDP log native VLAN mismatch
  Globally is disabled
  Per interface is enabled
gi1/0/1 is Down, CDP is enabled
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
```

show cdp neighbors

To display information about neighbors kept in the main or secondary cache, use the **show cdp neighbors** command in Privileged EXEC mode.

Syntax

show cdp neighbors [***interface-id***] [**detail** | **secondary**]

Parameters

- **interface-id**—Displays the neighbors attached to this port.
- **detail**—Displays detailed information about a neighbor (or neighbors) from the main cache including network address, enabled protocols, hold time, and software version.
- **secondary**—Displays information about neighbors from the secondary cache.

Default Configuration

If an interface ID is not specified, the command displays information for the neighbors of all ports.

If detail or secondary are not specified, a summary table of all neighbors is displayed.

Command Mode

Privileged EXEC mode

Example

switchxxxxxx# **show cdp neighbors**

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,P - VoIP Phone,
M - Remotely-Managed Device, C - CAST Phone Port, W - Two-Port MAC Relay
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - VoIP Phone
                  M - Remotely-Managed Device, C - CAST Phone Port,
                  W - Two-Port MAC Relay
    Device ID       Local      Adv  Time To Capability   Platform     Port ID
                    Interface  Ver. Live
------------------ ----------- ---- ------- ---------- ------------ -----------
PTK-SW-A-86.company   gi48       2     147      S I     Company        gi3/39
l.com                                                   XX-10R-E
    ESW-520-8P        gi48       2     153     S I M    ESW-520-8P     g1
    ESW-540-8P        gi48       2     146     S I M    ESW-540-8P     g9
   003106131611       gi48       2     143      S I     Company        fa2/1
                                                        XX-23R-E
   001828100211       gi48       2     173      S I     Company        fa2/2
                                                        XX-23R-E
    c47d4fed9302       gi48       2     137      S I    Company        fa2/5
                                                        XX-23R-E

switchxxxxxx# show cdp neighbors detail
-------------------------
Device ID: lab-7206
Advertisement version: 2
Entry address(es):
IP address: 172.19.169.83
Platform: company x5660, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): gi1/0/0
Time To Live : 123 sec
Version :
Company Network Operating System Software
NOS (tm) x5660 Software (D5660-I-N), Version 18.1(10.4), MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-1997 by company Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by xxdeeert
Duplex: half
-------------------------
Device ID: lab-as5300-1
Entry address(es):
IP address: 172.19.169.87
Platform: company TD6780, Capabilities: Router
Device ID: SEP000427D400ED
Advertisement version: 2
Entry address(es):
IP address: 1.6.1.81
Platform: Company IP Phone x8810, Capabilities: Host
Interface: gi1/0/1, Port ID (outgoing port): Port 1
Time To Live: 150 sec
Version :
```

```
P00303020204
Duplex: full
sysName: a-switch
Power drawn: 6.300 Watts

switchxxxxxx# show cdp neighbors secondary
Interface gi1/0/1, Port ID (outgoing port): gi2/0/20
MAC Address: 00:00:01:23:86:9c
Holdtime: 157
Capabilities: Router Switch
VLAN-ID: 10
Platform: 206VXRYC
Device-ID: 00000123869c
Addresses: IP 60.0.0.5, IPv6 2020::2020
nterface gi1/0/2, Port ID (outgoing port): gi2/0/21
MAC Address: 00:00:01:53:86:9c
Holdtime: 163
Capabilities: Router Switch
VLAN-ID: 10
Platform: ABCD-VSD
Device-ID: 00000153869c
Addresses: IP 61.0.0.4
Power Available: 30000
Request-ID: 1
Power management-ID: 234
Management-Power-Level is 0xFFFFFFFF
Interface gi1/0/3, Port ID (outgoing port): gi2/0/25
MAC Address: 00:00:22:23:86:9c
Holdtime: 144
Capabilities: Router Switch
VLAN-ID: 1210
Platform: bbbb
Device-ID: 00002223869c
Addresses: IP 70.0.0.4
4-wire Power-via-MDI (UPOE) TLV:
4-pair PoE Supported: Yes
Spare pair Detection/Classification required: Yes
PD Spare Pair Desired State: Disabled
PSE Spare Pair Operational State: Disabled
Power Available: 154000
Request-ID: 5
Power management-ID: 969
Management-Power-Level is 0xFFFFFFFF
Interface gi1/0/3, Port ID (outgoing port): gi1/0/11
MAC Address: 00:00:01:2c:86:9c
Holdtime: 120
Capabilities: Switch
VLAN-ID: 1005
Platform: CAT-3000
Device-ID: 0000012c869c
Addresses: IP 70.0.0.5
```

Field Definitions:

- **Advertisement version**—The version of CDP being used for CDP advertisements.
- **Capabilities**—The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
- **COS for Untrusted Ports**—The COS value with which all packets received on an untrusted port should be marked by a simple switching device which cannot itself classify individual packets.
- **Device ID**—The name of the neighbor device and either the MAC address or the serial number of this device.

- **Duplex**—The duplex state of connection between the current device and the neighbor device.
- **Entry address(es)**—A list of network addresses of neighbor devices.
- **Extended Trust**—The Extended Trust.
- **External Port-ID**—Identifies the physical connector port on which the CDP packet is transmitted. It is used in devices, such as those with optical ports, in which signals from multiple hardware interfaces are multiplexed through a single physical port. It contains the name of the external physical port through which the multiplexed signal is transmitted.
- **Interface**—The protocol and port number of the port on the current device.
- **IP Network Prefix**—It is used by On Demand Routing (ODR). When transmitted by a hub router, it is a default route (an IP address). When transmitted by a stub router, it is a list of network prefixes of stub networks to which the sending stub router can forward IP packets.
- **Management Address**—When present, it contains a list of all the addresses at which the device will accept SNMP messages, including those it will only accept when received on interface(s) other than the one over which the CDP packet is being sent.
- **MTU**—The MTU of the interface via which the CDP packet is sent.
- **Native VLAN**—The ID number of the VLAN on the neighbor device.
- **Physical Location**—A character string indicating the physical location of a connector which is on, or physically connected to, the interface over which the CDP packet containing this TLV is sent.
- **Platform**—The product name and number of the neighbor device. In the case of the Secondary Cache only the 8 last characters of the value are printed.
- **Power Available**—Every switch interface transmits information in the Power Available TLV, which permits a device which needs power to negotiate and select an appropriate power setting. The Power Available TLV includes four fields.
- **Power Consumption**—The maximum amount of power, in milliwatts, expected to be obtained and consumed from the interface over which the CDP packet is sent.
- **Power Drawn**—The maximum requested power.

  Note: For IP Phones the value shown is the maximum requested power (6.3 Watts). This value can be different than the actual power supplied by the routing device (generally 5 watts; shown using the show power command).
- **Protocol-Hello**—Specifies that a particular protocol has asked CDP to piggyback its "hello" messages within transmitted CDP packets.
- **Remote Port_ID**—Identifies the port the CDP packet is sent on
- **sysName**—An ASCII string containing the same value as the sending device's sysName MIB object.
- **sysObjectID**—The OBJECT-IDENTIFIER value of the sending device's sysObjectID MIB object.
- **Time To Live**—The remaining amount of time, in seconds, the current device will hold the CDP advertisement from a transmitting router before discarding it.
- **Version**—The software version running on the neighbor device.
- **Voice VLAN-ID**—The Voice VLAN-ID.

- **VTP Management Domain**—A string that is the name of the collective group of VLANs associated with the neighbor device.

show cdp tlv

To display information about TLVs sent by CDP on all ports or on a specific port, use the **show cdp tlv** command in Privileged EXEC mode.

Syntax

show cdp tlv [***interface-id***]

Parameters

interface-id—Port ID.

Default Configuration

TLVs for all ports.

Command Mode

Privileged EXEC mode

User Guidelines

You can use the **show cdp tlv** command to verify the TLVs configured to be sent in CDP packets. The **show cdp tlv** command displays information for a single port if specified or for all ports if not specified. Information for a port is displayed if only CDP is really running on the port, i.e. CDP is enabled globally and on the port, which is UP.

Example 1 - In this example, CDP is disabled and no information is displayed.

```
switchxxxxxx# show cdp tlv
cdp globally is disabled
```

Example 2 - In this example, CDP is globally enabled but disabled on the port and no information is displayed.

```
switchxxxxxx# show cdp tlv gi1/0/2
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/2
CDP is disabled on gi1/0/2
```

Example 3 - In this example, CDP is globally enabled and enabled on the port, but the port is down and no information is displayed.

```
switchxxxxxx# show cdp tlv interface gi1/0/2
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
```

```
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/3
CDP is enabled on gi1/0/3
Ethernet gi1/0/3 is down
```

Example 4 - In this example, CDP is globally enabled, and no ports are specified, so information is displayed for all ports on which CDP is enabled who are up.

```
switchxxxxxx# show cdp tlv interface
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/1
CDP is enabled
Ethernet gi1/0/1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4:  1.2.2.2 IPv6:
Port_ID TLV: gi1/0/1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
4-wire Power-via-MDI (UPOE) TLV:
                     4-pair PoE Supported: No
Power Available TLV: Request-ID is 1 Power management-ID is 1;
                                     Available-Power is 15.4;
                                     Management-Power-Level is 0xFFFFFFFF
Interface TLV: gi1/0/2
CDP is disabled on gi1/0/2
Interface TLV: gi1/0/3
CDP is enabled on gi1/0/3
Ethernet gi1/0/3 is down
```

Example 5 - In this example, CDP is globally enabled and enabled on the PSE PoE port, which is up and information is displayed.

```
switchxxxxxx# show cdp tlv interface gi1/0/1
cdp globally is enabled
Capability Codes: R - Router,T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
P - VoIP Phone,M - Remotely-Managed Device,
C - CAST Phone Port, W - Two-Port MAC Relay
Interface TLV: gi1/0/1
CDP is enabled
Ethernet gi1/0/1 is up,
Device ID TLV: type is MAC address; Value is 00:11:22:22:33:33:44:44
Address TLV: IPv4:  1.2.2.2 IPv6:
Port_ID TLV: gi1/0/1
Capabilities: S, I
Version TLV: 1 and 2
Platform TLV: VSD Ardd
Native VLAN TLV: 1
Full/Half Duplex TLV: full-duplex
Appliance VLAN_ID TLV: Appliance-ID is 1; VLAN-ID is 100
COS for Untrusted Ports TLV: 1
sysName: a-switch
Power Available TLV: Request-ID is 1 Power management-ID is 1;
                                     Available-Power is 15.4;
                                     Management-Power-Level is 0xFFFFFFFF
```

```
4-wire Power-via-MDI (UPOE) TLV:
                     4-pair PoE Supported: Yes
                     Spare pair Detection/Classification required: Yes
                     PD Spare Pair Desired State: Disabled
                     PSE Spare Pair Operational State: Disabled
Request-ID is 1 Power management-ID is 1;
                                      Available-Power is 15.4;
                                      Management-Power-Level is 0xFFFFFFFF
```

show cdp traffic

To display the CDP counters, including the number of packets sent and received and checksum errors, use the **show cdp traffic** command in Privileged EXEC mode.

Syntax

show cdp traffic [**global |** *interface-id*]

Parameters

- **global**—Display only the global counters
- ***interaface-id***—Port for which counters should be displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command **show cdp traffic** without parameters to display all the counters.

Use the **show cdp traffic global** to display only the global counters.

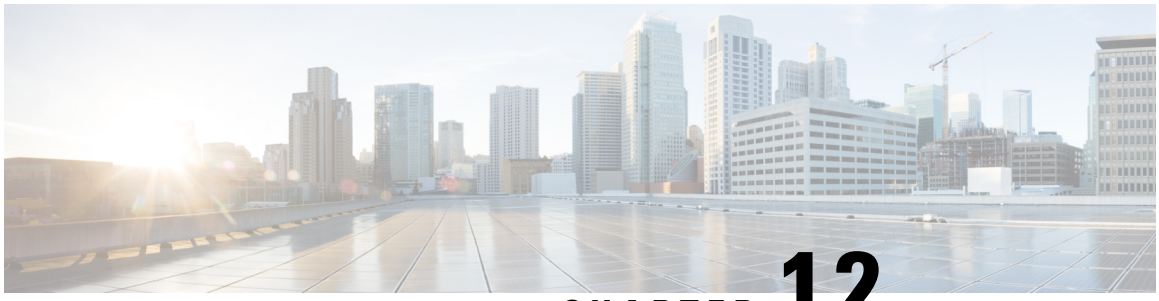
Use the **show cdp traffic** *interface-id* command to display the counters of the given port.

Example

```
switchxxxxxx# show cdp traffic
CDP Global counters:
     Total packets output: 81684,  Input: 81790
     Hdr syntax:  0, Chksum error: 0, Invalid packet: 0
     No memory in main cache: 0, in secondary cache: 0
     CDP version 1 advertisements output:  100,    Input  0
     CDP version 2 advertisements output:  81784,  Input  0
gi1/0/1
     Total packets output: 81684,  Input: 81790
     Hdr syntax:  0, Chksum error: 0, Invalid packet: 0
     No memory in main cache: 0, in secondary cache: 0
     CDP version 1 advertisements output:  100,    Input  0
     CDP version 2 advertisements output:  81784,  Input  0
gi1/0/2
     Total packets output: 81684,  Input: 81790
     Hdr syntax:  0, Chksum error: 0, Invalid packet: 0
     No memory in main cache: 0, in secondary cache: 0
     CDP version 1 advertisements output:  100,    Input  0
     CDP version 2 advertisements output:  81784,  Input  0
```

Field Definition:

- **Total packets output**—The number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
- **Input**—The number of CDP advertisements received by the local device. Note that this value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.
- **Hdr syntax**—The number of CDP advertisements with bad headers, received by the local device.
- **Chksum error**—The number of times the checksum (verifying) operation failed on incoming CDP advertisements.
- **No memory**—The number of times the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
- **Invalid**—The number of invalid CDP advertisements received.
- **CDP version 1 advertisements output** — The number of CDP Version 1 advertisements sent by the local device.
- **CDP version 1 advertisements Input**—The number of CDP Version 1 advertisements received by the local device.
- **CDP version 2 advertisements output**—The number of CDP Version 2 advertisements sent by the local device.
- **CDP version 2 advertisements Input**—The number of CDP Version 2 advertisements received by the local device.



CHAPTER 12

Clock Commands

This chapter contains the following sections:

- absolute, on page 207
- clock dhcp timezone, on page 208
- clock set, on page 209
- clock source, on page 210
- clock summer-time, on page 211
- clock timezone, on page 212
- periodic, on page 213
- sntp anycast client enable, on page 214
- sntp authenticate, on page 215
- sntp authentication-key, on page 215
- sntp broadcast client enable, on page 216
- sntp client enable, on page 217
- sntp client enable (interface), on page 217
- sntp server, on page 218
- sntp source-interface, on page 219
- sntp source-interface-ipv6, on page 220
- sntp trusted-key, on page 220
- sntp unicast client enable, on page 221
- sntp unicast client poll, on page 222
- show clock, on page 222
- show sntp configuration, on page 224
- show sntp status, on page 224
- show time-range, on page 225
- time-range, on page 226

absolute

To specify an absolute time when a time range is in effect, use the **absolute** command in Time-range Configuration mode. To restore the default configuration, use the **no** form of this command.

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: 2020–2037)

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
```

clock dhcp timezone

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 **clock dhcp timezone** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

clock dhcp timezone

no clock dhcp timezone

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

- 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 interface.

Example

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

clock set

To set the system clock manually, use the **clock set** command in Privileged EXEC mode.

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: 2020–2037)

Default Configuration

The time of the image creation.

Command Mode

Privileged EXEC mode

User Guidelines

After boot the system clock is set to the time of the image creation.

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
```

clock source

To configure an external time source for the system clock, use the **clock source** command in Global Configuration mode. To disable the external time source, use the **no** form of this command.

Syntax

clock source {**sntp | browser***}*

no clock source {**sntp | browser***}*

Parameters

- **sntp**—(Optional) Specifies that an SNTP server is the external clock source.
- **browser**—(Optional) 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

SNTP

Command Mode

Global Configuration mode

User Guidelines

After boot the system clock is set to the time of the image creation.

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

if the command is executed twice, each time with a different clock source, both sources will be operational, SNTP has higher priority than time from browser.

Example

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

```
switchxxxxxx(config)# clock source sntp
switchxxxxxx(config)# clock source browser
switchxxxxxx(config)# exit
switchxxxxxx# show clock
*10:46:48 UTC May 28 2013
Time source is sntp
Time from Browser is enabled
```

clock summer-time

To configure the system to automatically switch to summer time (Daylight Saving Time), use the **clock summer-time** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

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. (Range: 1- 4 characters). Only letters can be included in the acronym.
- **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 1–5, first to 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: 2020–2037)
- ***hh:mm***—Time (military format) in hours and minutes. (Range: hh:mmhh: 0-23, mm: 0-59)
- ***offset***—(Optional) 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
```

clock timezone

To set the time zone for display purposes, use the **clock timezone** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

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

no clock timezone

Parameters

- ***zone***—The acronym of the time zone. (Range: 1- 4 characters). Only letters can be included in the acronym.
- ***hours-offset***—Hours difference from UTC. (Range: (-12)–(+13))

- ***minutes-offset***—(Optional) Minutes difference from UTC. (Range: 0–59)

Default Configuration

Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), which is the same:

- 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
```

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in Time-range Configuration mode. To restore the default configuration, use the **no** form of this command.

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 *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
```

sntp anycast client enable

To enable the SNTP Anycast client, use the **sntp anycast client enable** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp anycast client enable *[***both** | **ipv4** | **ipv6***]*

Parameters

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

sntp authenticate

To enable authentication for received SNTP traffic from servers, use the **sntp authenticate** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp authenticate

no sntp authenticate

Default Configuration

Authentication is disabled.

Command Mode

Global Configuration mode

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
```

sntp authentication-key

To define an authentication key for Simple Network Time Protocol (SNTP), use the **sntp authentication-key** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp authentication-key *key-number* **md5| sha1| sha2-256| hmac-sha2-256** *key-value*

encrypted sntp authentication-key *key-number* **md5** encrypted-*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)
- ***encrypted-key-value***—Specifies the key value in encrypted format.

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
```

sntp broadcast client enable

To enable SNTP Broadcast clients, use the **sntp broadcast client enable** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp broadcast client enable *[***both** | **ipv4** | **ipv6***]*

no sntp broadcast client enable

Parameters

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

Example

The following example enables SNTP Broadcast clients.

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

sntp client enable

To enable the SNTP Broadcast and Anycast client, use the **sntp client enable** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

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.

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp client enable** command to enable SNTP Broadcast and Anycast clients.

Example

The following example enables the SNTP Broadcast and Anycast clients on VLAN 100:

```
switchxxxxxx(config)# sntp client enable vlan 100
```

sntp client enable (interface)

To enable the SNTP Broadcast and Anycast client on an interface, use the **sntp client enable** command in Interface Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp client enable

no sntp client enable

Default Configuration

The SNTP client is disabled on an interface.

Command Mode

Interface Configuration mode

User Guidelines

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

Example

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

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# sntp client enable
switchxxxxxx(config-if)# exit
```

sntp server

To configure 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 **sntp server** command in Global Configuration mode. To remove a server from the list of SNTP servers, use the **no** form of this command.

Syntax

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

no sntp server [*ip-address* | *hostname*]

Parameters

- **default**—Default defined SNTP servers.
- ***ip-address***—Specifies the server IP address. This can be an IPv4, IPv6 or IPv6z address.
- ***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**—(Optional) Enables polling.
- **key** *keyid*—(Optional) Specifies the Authentication key to use when sending packets to this peer. (Range:1–4294967295)

Default Configuration

The following servers with polling and without authentication are defined:

- ***time-a.timefreq.bldrdoc.gov***
- ***time-b.timefreq.bldrdoc.gov***
- ***time-c.timefreq.bldrdoc.gov***
- ***pool.ntp.org***
- ***time-pnp.cisco.com***

Command Mode

Global Configuration mode

User Guidelines

Use the **sntp server** {***ip-address*** | ***hostname***} [**poll**] [**key** ***keyid***] command to define a SNTP server. The switch supports up to 8 SNTP servers.

Use the **sntp server default** command to return to the default configuration.

Use the **no sntp server** *ip-address* | *hostname* command to remove one SNTP server.

Use the **no sntp server** to remove all SNTP servers.

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
```

sntp source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SNTP servers, use the **sntp source-interface** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp source-interface *interface-id*

no sntp source-interface

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SNTP server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sntp source-interface vlan 10
```

sntp source-interface-ipv6

To specify the source interface whose IPv6 address will be used ad the Source IPv6 address for communication with IPv6 SNTP servers, use the **sntp source-interface-ipv6** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

sntp source-interface-ipv6 *interface-id*

no sntp source-interface-ipv6

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

The outgoing interface is selected based on the SNTP server's IP address. If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SNTP server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sntp source-interface-ipv6 vlan 10
```

sntp trusted-key

To define the trusted key, use the **sntp trusted-key** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

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 trusted key is used for authentication of all servers not having personal keys assigned.

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
```

sntp unicast client enable

To enable the device to use Simple Network Time Protocol (SNTP) Unicast clients, use the **sntp unicast client enable** command in Global Configuration mode. To disable the SNTP Unicast clients, use the **no** form of this command.

Syntax

sntp unicast client enable

no sntp unicast client enable

Default Configuration

The SNTP unicast clients are enabled.

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
```

sntp unicast client poll

To enable polling for the SNTP Unicast clients, use the **sntp unicast client poll** command in Global Configuration mode. To disable the polling, use the **no** form of this command.

Syntax

sntp unicast client poll

no sntp unicast client poll

Default Configuration

Polling is enabled.

Command Mode

Global Configuration mode

User Guidelines

The polling interval is 1024 seconds.

Example

The following example enables polling for SNTP unicast clients.

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

show clock

To display the time and date from the system clock, use the **show clock** command in User EXEC mode.

Syntax

show clock [**detail**]

Parameters

- **detail**—(Optional) Displays the time zone and summer time configuration.

Command Mode

User EXEC mode

User Guidelines

The default output of the command shows the current system date and time, information on the operational source of the system time and general clock related configurations.

The detailed output of the command shows additional information about time-zone and daylight savings configuration.

The possible values for operational system time source are:

- RTC - Indicates that the system time was set from the Real Time Clock component. This happens if the system clock hasn't been set by SNTP, by a user or by the browser.
- User - If the system clock was last set manually by a user.
- SNTP - if the system clock was last set by SNTP. In this case, the time since the last synchronization with the SNTP server is also displayed.
- None - If the clock hasn't been set by any method since the last reboot and the system does not have an RTC component.

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

```
switchxxxxxx# show clock
 15:29:03 PDT(UTC-7) Jun 17 2019
Operational Time Source: SNTP (last synchronized 2 days, 18 hours, 29 minutes and 3 seconds
 ago)
Time from SNTP is enabled
Time from Browser is disabled
```

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

```
switchxxxxxx# show clock detail
 15:22:55 SUN Apr 23 2019
Operational Time Source: User
Time from SNTP is disabled
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
```

show sntp configuration

To display the SNTP configuration on the device, use the **show sntp configuration** command in Privileged EXEC mode.

Syntax

show sntp configuration

Command Mode

Privileged EXEC mode

Examples

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

```
switchxxxxxx# show sntp configuration
SNTP port : 123
Polling interval: 04 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_server1.comapany.com
  Polling: enabled
  Encryption Key: disabled
Server: dns_server2.comapany.com
  Polling: enabled
  Encryption Key: disabled
Broadcast Clients: enabled for IPv4 and IPv6
Anycast Clients: disabled
No Broadcast Interfaces
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
```

show sntp status

To display the SNTP servers status, use the **show sntp status** command in Privileged EXEC mode.

Syntax

show sntp status

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 2015
  Last request: 19:58:21.555 PDT Feb 19 2015
  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 2015
  Last request: 12:58:21.555 PDT Feb 19 2015
  Stratum Level: 1
  Offset: 8.98mSec
  Delay: 189.19mSec
Server: 3001:1:1::1
  Source: DHCPv6 on VLAN 2
  Status: Unknown
  Last response:
  Last request:
  Offset: mSec
  Delay: mSec
Server: dns1.company.com
  Source: DHCPv6 on VLAN 20
  Status: Unknown
  Last response:
  Last request:
  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
  Last request: 9:53:21.689 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
  Last reqeust: 9:53:21.689 PDT Feb 19 2005
  Stratum Level: 255
```

show time-range

To display the time range configuration, use the **show time-range** command in User EXEC mode.

Syntax

show time-range *time-range-name*

Parameters

- ***time-range-name***—Specifies the name of an existing time range.

Command Mode

User 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
```

time-range

To define time ranges and to enter to Time-range Configuration mode, use the **time-range** command to define time ranges and to enter to Time-range Configuration mode in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

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 entering to Time-range Configuration mode 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.

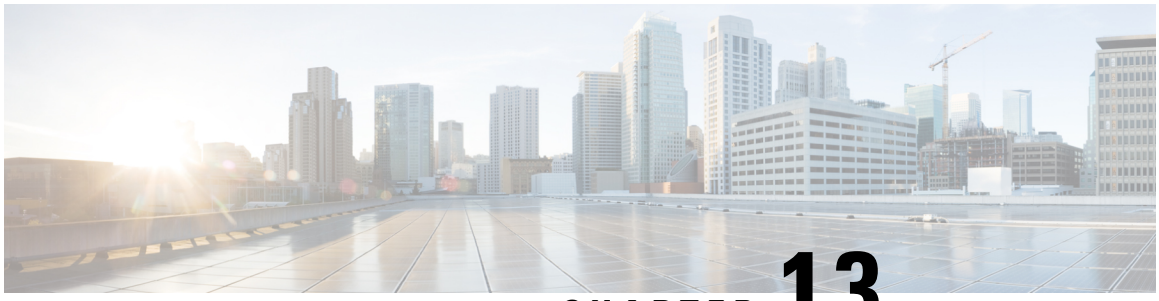
If a **time-range** command has both absolute and periodic values specified, then the periodic items are evaluated only after the absolute start time is reached, and are not evaluated again after the absolute end time is reached.

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 is not activated.

Example

```
switchxxxxxx(config)# time-range http-allowed
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
```



CHAPTER 13

DHCP Relay Commands

This chapter contains the following sections:

- ip dhcp relay enable (Global), on page 229
- ip dhcp relay enable (Interface), on page 230
- ip dhcp relay address (Global), on page 230
- show ip dhcp relay, on page 231
- ip dhcp information option, on page 232
- ip dhcp information option numeric-token-format, on page 232
- ip dhcp information option circuit-id, on page 233
- ip dhcp information option remote-id, on page 237
- show ip dhcp information option tokens, on page 241
- show ip dhcp information option , on page 243

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

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
```

ip dhcp relay enable (Interface)

Use the **ip dhcp relay enable** Interface Configuration 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

Default Configuration

Disabled

Command Mode

Interface Configuration 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
```

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
```

show ip dhcp relay

Use the **show ip dhcp relay** EXEC mode command to display the DHCP relay information.

Syntax

show ip dhcp relay

Command Mode

User EXEC mode

Examples

Option 82 is disabled:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally disabled
Option 82 is disabled
Maximum number of supported VLANs without IP Address: 0
Number of DHCP Relays enabled on VLANs without IP Address: 4
DHCP relay is enabled on Ports: gi1/0/1,po1-2
 Active:
 Inactive: gi1/0/1, po1-4
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active:
 Inactive: 1, 2, 4, 5
Global Servers: 1.1.1.1 , 2.2.2.2
```

Option 82 is enabled:

```
switchxxxxxx# show ip dhcp relay
DHCP relay is globally enabled
Option 82 is enabled
Maximum number of supported VLANs without IP Address is 4
```

```
Number of DHCP Relays enabled on VLANs without IP Address: 2
DHCP relay is enabled on Ports: gi1/0/1,po1-2
 Active: gi1/0/1
 Inactive: po1-2
DHCP relay is enabled on VLANs: 1, 2, 4, 5
 Active: 1, 2, 4, 5
 Inactive:
Global Servers: 1.1.1.1 , 2.2.2.2
```

ip dhcp information option

Use the **ip dhcp information option** Global Configuration mode 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

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
```

ip dhcp information option numeric-token-format

Use the **ip dhcp information option numeric-token-format** Global Configuration mode command to define the format of numeric tokens included in the Circuit-ID and Remote-ID sub-options payload template. Use the **no** form of this command to return to default format.

Syntax

ip dhcp information option numeric-token-format {hex|ascii}

no ip dhcp information option numeric-token-format

Parameters

- **hex** - Hexadecimal (Numeric value) format will be used in packet for numeric token included in the Circuit-ID and Remote-ID payload template.

- **ascii** - ASCII format will be used in packet for numeric token included in the Circuit-ID and Remote-ID payload template. If this option is selected, each individual digit in a numeric token will be represented by its value in the ASCII table.

Default Configuration

The default format used is the hexadecimal/numeric format

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure the format of numeric token included in the Circuit-ID or Remote-ID sub-options payload templates commands: ip dhcp information option circuit-id and ip dhcp information option remote-id.

The following are the numeric tokens affected by this command:

- $int-ifindex$
- $int-portid$
- $switch-moduleid$
- $vlan-id$

Example

The following example configures the device to use the ASCII format for insertion of numeric-tokens:

```
switchxxxxxx(config)# ip dhcp information option numeric-token-format ascii
```

ip dhcp information option circuit-id

Use the **ip dhcp information option circuit-id** Global Configuration mode command to configure the template of DHCP option 82 Circuit-ID sub-option payload. Use the **no** form of this command to return to default template.

Syntax

ip dhcp information option circuit-id *text*

no ip dhcp information option circuit-id

Parameters

- ***text*** - Concatenation of free text and one or more tokens in the format of $tokenname$ (length 1-160).

Default Configuration

The default Circuit-ID payload template is *$vlan-id$$switch-moduleid$$int-portid$*

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure the template of the option 82 Circuit-ID sub-option payload, inserted by device. The payload section of the Circuit-ID sub option includes all bytes of sub option besides the first 4 bytes of the sub option which values are set by device as follows:

Circuit ID sub option Type (value = 1)

- Sub option total length (not including 1st byte and total length byte)

  Circuit ID type (value= 1); Note: if default sub option template is used - value of this field equals 0

  Sub option payload length

The *text* field is a concatenation of free text and one or more tokens in the format of *$tokenname$*. Tokens must be entered in the exact format specified (see table below) or it will not be recognized as a token

The *text* can begin or end with free text or a token. Tokens can be concatenated sequentially or separated by free text. If the free text includes a space character - the *text* parameter must be placed between quotation (e.g. "*text1 text2*").

The Circuit-ID payload template must include at least 1 token related to an interface parameter (token beginning with *$int-xxx$*). In addition - if the string does not include a VLAN related token - user will be asked to confirm setting.

The total length of the *text* field in the command cannot exceed 160 bytes. The byte count includes all bytes of the text parameter - including all free text and Tokens as written in the *text* field.

The combined length of the Circuit-ID payload Remote-ID payload cannot exceed 247 bytes. The payload byte count takes into account the count of free-text chars (1 byte each) and a predefined length reserved for each token (see in table below).

The following table details supported tokens, the device parameter they represent and the reserved and actual byte count per each token:

Token Name	Description	Reserved Length	Actual Length
$int-ifindex$	Source interface ifIndex value	4 bytes	Hex Format - 2 bytes ASCII format - 4 bytes
$int-portid$	Source interface sequential number on the specific module (in stack). For LAG source interfaces - it is the LAG ID	2 bytes	Hex Format - 1 bytes ASCII format - 2 bytes
$int-name$	The full name of the source interface, as used in CLI commands	32 bytes	The actual number of bytes needed for ASCII representation of the interface full name

Token Name	Description	Reserved Length	Actual Length
$int-abrvname$	The abbreviated name of the source interface, as used in CLI commands	8 bytes	The actual number of bytes needed for ASCII representation of the interface full name
$int-desc-16$	The description configured by user on source interface. If description is more than 16 bytes - only the 1st 16 bytes are used If a description is not configured, the abbreviated interface name is used	16 bytes	The actual number of bytes needed for ASCII representation of the interface description (max 16 bytes)
$int-desc-32$	The description configured by user on source interface. If description is more than 32 bytes - only the 1st 32 bytes are used If a description is not configured, the abbreviated interface name is used	32 bytes	The actual number of bytes needed for ASCII representation of the interface description (max 32 bytes)
$int-desc-64$	The description configured by user on source interface. If a description is not configured, the abbreviated interface name is used	64 bytes	The actual number of bytes needed for ASCII representation of the interface description
$int-mac$	MAC address of the source interface (Hex value with no delimiter)	6 bytes	6 bytes
$switch-mac$	MAC address of the switch relaying/forwarding DHCP packet (Hex value with no delimiter)	6 bytes	6 bytes

Token Name	Description	Reserved Length	Actual Length
$switch-hostname-16$	The hostname of the switch relaying/forwarding DHCP packet. If the hostname is more than 16 bytes - only the 1st 16 bytes are used	16 bytes	The actual number of bytes needed for ASCII representation of the hostname (max 16 bytes)
$switch-hostname-32$	The hostname of the switch relaying/forwarding DHCP packet. If the hostname is more than 32 bytes - only the 1st 32 bytes are used	32 bytes	The actual number of bytes needed for ASCII representation of the hostname (max 32 bytes)
$switch-hostname-58$	The hostname of the switch relaying/forwarding DHCP packet.	58 bytes	The actual number of bytes needed for ASCII representation of the hostname
$switch-moduleid$	The unit ID of the source interface upon which the DHCP client request was received	2 bytes	Hex Format - 1 bytes ASCII format - 2 bytes
$vlan-id$	The Source VLAN ID (1-4094)	4 bytes	Hex Format - 2 bytes ASCII format - 4 bytes
$vlan-name-16$	The VLAN name assigned by user to the VLAN. If the name is more than 16 bytes - only the 1st 16 bytes are used If a name is not configure for the VLAN, the value is taken from the relevant VLAN ifDescr MIB field	16 bytes	The actual number of bytes needed for ASCII representation of the VLAN name (max 16)
$vlan-name-32$	The VLAN name assigned by user to the VLAN. If a name is not configure for the VLAN, the value is taken from the relevant VLAN ifDescr MIB field	32 bytes	The actual number of bytes needed for ASCII representation of the VLAN name (max 32)

Notes:

- Source Interface or VLAN int table refers to the Interface or VLAN on which the DHCP client packet (to which the option 82 is added) was received on.
- Reserved (Byte) Length - The maximum length the token may "consume" in the packet. This value is used for calculation of the 247 byte limit (for all sub options payload combined). The reserved length does not change if numeric tokens are filled in as Hexadecimal or ASCII values.
- Actual (Byte) Length - The actual number of bytes the token will "consume" in packet itself. The actual byte length may change (for relevant tokens) if token is filled in as exadecimal or ASCII values.

Example

The following example configures the Circuit-ID payload template to a concatenation of free text and tokens representing interface name and VLAN name (up to 16 chars):

```
switchxxxxxx(config)# ip dhcp information option circuit-id aaa$int-name$bbb$vlan-name-16$ccc
```

The following example configures the Circuit-ID payload template to - where text parameter does not include a token related to an interface:

```
switchxxxxxx(config)# ip dhcp information option circuit-id aaa
Illegal Circuit-ID payload: Cicuit-ID must include at least 1 interface related Token
```

The following example configures the Circuit-ID payload template to use a concatenation of free text and tokens - where template does not include a token related to a VLAN:

```
switchxxxxxx(config)# ip dhcp information option circuit-id aaa$int-name$bbb
Circuit-ID payload does not include a token reflecting DHCP client source VLAN. Continue?
y/n[n] y
```

The following example configures the Circuit-ID payload template to use a concatenation of free text and tokens - resulting in a combined Circuit-ID and Remote-ID reserved payloads which exceed 247 bytes:

```
switchxxxxxx(config)# ip dhcp information option circuit-id
aaa$vlan-name-32$bbb$int-desc-64$ccc$switch-hostname-58$ddd
Illegal Circuit-ID payload: Circuit-ID and Remote-ID payload reserved byte count exceeds
247 bytes
```

ip dhcp information option remote-id

Use the **ip dhcp information option remote-id** Global Configuration mode command to configure the template of DHCP option 82 Remote-ID sub-option payload. Use the **no** form of this command to return to default template.

Syntax

ip dhcp information option remote-id *text*

no ip dhcp information option remote-id

Parameters

- ***text*** - concatenation of free text and one or more tokens in the format of $tokenname$ (length 1-160).

Default Configuration

The default Remote-ID payload template is *$switch-mac$*

Command Mode

Global Configuration mode

User Guidelines

Use this command to configure the template of the option 82 Remote-ID sub-option payload, inserted by device. The payload section of the Remote-ID sub option includes all bytes of sub option besides the first 4 bytes of the sub option which values are set by device as follows:

Remote-ID sub option Type (value = 2)

- Sub option total length (not including 1st byte and total length byte) Remote-ID type (value= 1); Note: if default sub option template is used - value of this field equals 0. Sub option payload length

The *text* field is a concatenation of free text and one or more tokens in the format of *$tokenname$*. Tokens must be entered in the exact format specified (see table below) or it will not be recognized as a token

The *text* can begin or end with free text or a token. Tokens can be concatenated sequentially or separated by free text. If the free text includes a space character - the *text* parameter must be placed between quotation (e.g. "*text1 text2*").

The Remote-ID payload template may include 1 token, multiple tokens or no tokens at all.

The total length of the *text* field in the command cannot exceed 160 bytes. The byte count includes all bytes of the text parameter - including all free text and Tokens as written in the *text* field.

The combined length of the Circuit-ID payload Remote-ID payload cannot exceed 247 bytes. The payload byte count takes into account the count of free-text chars (1 byte each) and a predefined length reserved for each token (see in table below).

The following table details supported tokens, the device parameter they represent and the reserved and actual byte count per each token:

Token Name	Description	Reserved Length	Actual Length
$int-ifindex$	Source interface ifIndex value	4 bytes	Hex Format - 2 bytes ASCII format - 4 bytes
$int-portid$	Source interface sequential number on the specific module (in stack). For LAG source interfaces - it is the LAG ID	2 bytes	Hex Format - 1 bytes ASCII format - 2 bytes
$int-name$	The full name of the source interface, as used in CLI commands	32 bytes	The actual number of bytes needed for ASCII representation of the interface full name

Token Name	Description	Reserved Length	Actual Length
$int-abrvname$	The abbreviated name of the source interface, as used in CLI commands	8 bytes	The actual number of bytes needed for ASCII representation of the interface full name
$int-desc-16$	The description configured by user on source interface. If description is more than 16 bytes - only the 1st 16 bytes are used If a description is not configured, the abbreviated interface name is used	16 bytes	The actual number of bytes needed for ASCII representation of the interface description (max 16 bytes)
$int-desc-32$	The description configured by user on source interface. If description is more than 32 bytes - only the 1st 32 bytes are used If a description is not configured, the abbreviated interface name is used	32 bytes	The actual number of bytes needed for ASCII representation of the interface description (max 32 bytes)
$int-desc-64$	The description configured by user on source interface. If a description is not configured, the abbreviated interface name is used	64 bytes	The actual number of bytes needed for ASCII representation of the interface description
$int-mac$	MAC address of the source interface (Hex value with no delimiter)	6 bytes	6 bytes
$switch-mac$	MAC address of the switch relaying/forwarding DHCP packet (Hex value with no delimiter)	6 bytes	6 bytes

Token Name	Description	Reserved Length	Actual Length
$switch-hostname-16$	The hostname of the switch relaying/forwarding DHCP packet. If the hostname is more than 16 bytes - only the 1st 16 bytes are used	16 bytes	The actual number of bytes needed for ASCII representation of the hostname (max 16 bytes)
$switch-hostname-32$	The hostname of the switch relaying/forwarding DHCP packet. If the hostname is more than 32 bytes - only the 1st 32 bytes are used	32 bytes	The actual number of bytes needed for ASCII representation of the hostname (max 32 bytes)
$switch-hostname-58$	The hostname of the switch relaying/forwarding DHCP packet.	58 bytes	The actual number of bytes needed for ASCII representation of the hostname
$switch-moduleid$	The unit ID of the source interface upon which the DHCP client request was received	2 bytes	Hex Format - 1 bytes ASCII format - 2 bytes
$vlan-id$	The Source VLAN ID (1-4094)	4 bytes	Hex Format - 2 bytes ASCII format - 4 bytes
$vlan-name-16$	The VLAN name assigned by user to the VLAN. If the name is more than 16 bytes - only the 1st 16 bytes are used If a name is not configure for the VLAN, the value is taken from the relevant VLAN ifDescr MIB field	16 bytes	The actual number of bytes needed for ASCII representation of the VLAN name (max 16)
$vlan-name-32$	The VLAN name assigned by user to the VLAN. If a name is not configure for the VLAN, the value is taken from the relevant VLAN ifDescr MIB field	32 bytes	The actual number of bytes needed for ASCII representation of the VLAN name (max 32)

Notes:

- Source Interface or VLAN int table refers to the Interface or VLAN on which the DHCP client packet (to which the option 82 is added) was received on.
- Reserved (Byte) Length - The maximum length the token may “consume” in the packet. This value is used for calculation of the 247 byte limit (for all sub options payload combined). The reserved length does not change if numeric tokens are filled in as Hexadecimal or ASCII values.
- Actual (Byte) Length - The actual number of bytes the token will “consume” in packet itself. The actual byte length may change (for relevant tokens) if token is filled in as hexadecimal or ASCII values.

Example

The following example configures the device to use a Remote-ID which is a concatenation of free text and the full device hostname:

```
switchxxxxxx(config)# ip dhcp information option remote-id aaa$switch-hostname-58$bbb
```

show ip dhcp information option tokens

Use the **show ip dhcp information option tokens** User EXEC mode command to display tokens which can be used when configuring the payloads of Circuit-ID and Remote-ID sub options (DHCP option 82):

Syntax

show ip dhcp information option tokens [brief]

Parameters

- **Brief** - Displays the name of the tokens without token information.

Default Configuration

Full token information is displayed

Command Mode

User EXEC mode

User Guidelines

Use this command to display the tokens that can be used as part of the text parameter in commands ip dhcp information option circuit-id or ip dhcp information option remote-id. The tokens represent various system info, which the user can include in either of the sub-options’ payloads. This allows automatic update of value based on current system information and also based on relevant interfaces.

The tokens have meaningful and pre-determined names based on the information they represent. A $ symbol is placed before and after the Token name ($token-name$).

Tokens can be divided, in general, into 3 groups: Tokens which represent interface level information (format of $int-xxx$); Tokens which represent switch level information (format of $switch-xxx$), and tokens which represent VLAN related information (format of $vlan-xxx$).

Example

The following example displays all supported tokens and all the information related to each token:

```
switchxxxxxx# show ip dhcp information option tokens
Interface level Tokens - relates to the interface upon which the DHCP client packet was
received:
Token Name: $int-ifindex$
Token value: ifIndex of the interface
Token format: Hex (default) or ASCII
Token reserved length: 4 bytes.
Token actual payload length: 2(HEX)/4(ASCII) bytes.
Token Name: $int-portid$
Token value: interface number relative to the specific unit (standalone or stacking unit)
Token format: Hex (default) or ASCII
Token reserved length: 2 bytes
Token actual payload length: 1(HEX)/2(ASCII) bytes
Token Name: $int-name$
Token value: The interface full name based as used in CLI
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-abrvname$
Token value: The interface abbreviated name as used in CLI
Token format: ASCII
Token reserved length: 8 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-desc-16$
Token value: (up to) The first 16 bytes of the description user configured for the interface
Token format: ASCII
Token reserved length: 16 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-desc-32$
Token value: (up to) The first 32 bytes of the description user configured for the interface
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-desc-64$
Token value: The full description user configured for the interface (even if more than 32
bytes)
Token format: ASCII
Token reserved length: 64 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $int-mac$
Token value: The MAC address of the physical interface
Token format: HEX
Token reserved length: 6 bytes
Token actual payload length:6 bytes
Device level Tokens - relates to switch level information:
Token Name: $switch-mac$
Token value: Device base MAC address
Token format: HEX
Token reserved length: 6 bytes
Token actual payload length:6 bytes
Token Name: $switch-hostname-16$
Token value: (Up to) The first 16 bytes of the hostname of the device
Token format: ASCII
Token reserved length: 16 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $switch-hostname-32$
Token value: (Up to) The first 32 bytes of the hostname of the device
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $switch-hostname-58$
```

```
Token value: Device full hostname (even if more than 32 bytes)
Token format: ASCII
Token reserved length: 58 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $switch-moduleid$
Token value: The unit ID of the unit within the stack
Token format: Hex (default) or ASCII
Token reserved length: 2 bytes
Token actual payload length: 1(HEX)/2(ASCII) bytes
VLAN level Tokens - relates to the VLAN upon which the DHCP client packet was received:
Token Name: $vlan-id$
Token value: VLAN ID (1-4094)
Token format: Hex (default) or ASCII
Token reserved length: 4 bytes
Token actual payload length: 2(HEX)/4(ASCII) bytes
Token Name: $vlan-name-16$
Token value: (Up to) The first 16 bytes of the VLAN name
Token format: ASCII
Token reserved length: 16 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
Token Name: $vlan-name-32$
Token value: The full VLAN name (even if more than 16 bytes)
Token format: ASCII
Token reserved length: 32 bytes
Token actual payload length: Actual number of bytes (ASCII) inserted to sub-option
```

The following example displays only the names of the supported Tokens:

```
switchxxxxxx# show ip dhcp information option tokens brief
Interface level Tokens:
$int-ifindex$
$int-portid$
$int-name$
$int-abrvname$
$int-desc-16$
$int-desc-32$
$int-desc-64$
$int-mac$
Device level Tokens:
$switch-mac$
$switch-hostname-16$
$switch-hostname-32$
$switch-hostname-58$
$switch-moduleid$
VLAN level Tokens:
$vlan-id$
$vlan-name-16$
$vlan-name-32$
```

show ip dhcp information option

The **show ip dhcp information option** User EXEC mode command displays the DHCP Option 82 and sub option configuration.

Syntax

show ip dhcp information option [{interface *interface-id***} {vlan** *vlan***}]**

Parameters

- **interface** *interface-id* - Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel. Use this parameter together with the **vlan** parameter to display actual option 82 payload for a DHCP client message received on the specified interface and VLAN
- **vlan** *vlan*- Specifies a VLAN ID Use this parameter together with the **interface** parameter to display actual option 82 payload for a DHCP client message received on the specified interface and VLAN

Default Configuration

If no parameter is entered the general settings of option 82 will be displayed.

Command Mode

User EXEC mode

Example

The following example displays global information for DHCP option 82, including sub options, when user did not change the settings of Option 82 sub-options.

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: (default)
Remote-id payload template: (default)
Total sub Options reserved payload: 14/247 bytes
```

The following example displays global information for DHCP option 82, including sub options, where user modified both Circuit-ID and Remote-ID sub-options.

```
switchxxxxxx# show ip dhcp information option
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: aaa$int-name$bbb$vlan-name$ccc
Remote-id payload template: aaa$switch-hostname-58$bbb
Total sub Options reserved payload: 143/247 bytes
```

The following example displays specific interface and VLAN information for DHCP option 82, where user modified both Circuit-ID and Remote-ID sub-options.

```
switchxxxxxx# show ip dhcp information option interface te1/0/1 vlan 2
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: aaa$int-name$bbb$vlan-name$ccc
Remote-id payload template: aaa$switch-hostname-58$bbb
Total sub Options reserved payload: 143/247 bytes
Interface te1/0/1 vlan 2:
Circuit-id header content: 0131012f
Circuit-id payload content: 61616154656e67696761626974457461865726e657431
2f302f3162626241502d564c414e636363
Circuit-id payload textual resolution: aaaTengigabitEthernet1/0/1bbbAP-VLANccc //removed
support 31-Jul-18//
Circuit-id Total Length: 43
Remote-id header content: 0211010f
Remote-id payload content: 616161466c6f6f72345377697461368626262
Remote-id payload textual resolution: aaaFloor4Switchbbbb //removed support 31-Jul-18//
Remote-id Total Length: 22
```

The following example displays specific interface and VLAN information for DHCP option 82, including sub options, when user modified only the Circuit-ID sub-option.

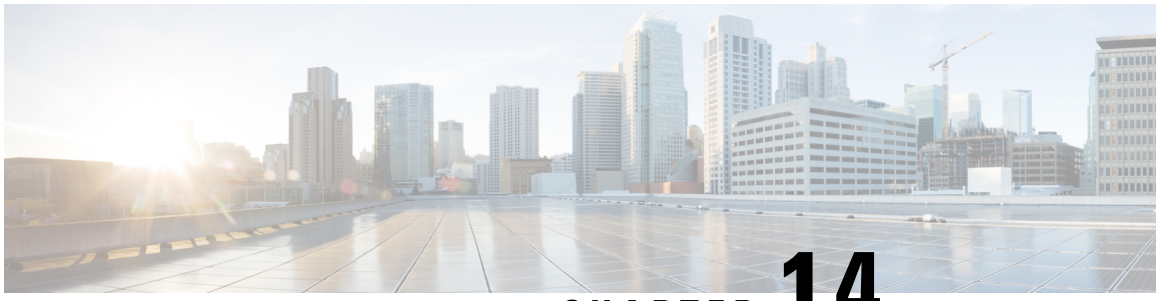
```
switchxxxxxx# show ip dhcp information option interface te1/0/10 vlan 13
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: $int-portid$aaa$vlan-id$zzz
Remote-id payload template: (default)
Total sub Options reserved payload: 18/247 bytes
Interface te1/0/10 vlan 13:
Circuit-id header content: 010b012f
Circuit-id payload content: 0a616161000d7a7a7a
Circuit-id payload textual resolution: 10aaa13zzz //removed support 31-Jul-18//
Circuit-id Total Length: 13
Remote-id header content: 02080006
Remote-id payload content: 000000112233
Remote-id payload textual resolution: 000000112233 //removed support 31-Jul-18//
Remote-id Total Length: 10
```

The following example displays specific interface and VLAN information for DHCP option 82, when user set Numeric Token format to ASCII and configured Circuit-ID sub-option.

```
switchxxxxxx# show ip dhcp information option interface te1/0/10 vlan 13
Relay agent Information option is Enabled
Numeric Token format: ascii
Circuit-id payload template: $int-portid$aaa$vlan-id$zzz
Remote-id payload template: (default)
Total sub Options reserved payload: 18/247 bytes
Interface te1/0/10 vlan 13:
Circuit-id header content: 010e012f
Circuit-id payload content: 3130616161303031337a7a7a
Circuit-id payload textual resolution: 10aaa13zzz ////removed support 31-Jul-18//
Circuit-id Total Length: 16
Remote-id header content: 0211000f
Remote-id payload content: 000000112233
Remote-id payload textual resolution: 000000112233 //removed support 31-Jul-18//
Remote-id Total Length: 10
```

The following example requested display is for specific interface and VLAN information for DHCP option 82, where $vlan-name-32$ is one of the tokens - but the specific VLAN was not created on device.

```
switchxxxxxx# show ip dhcp information option interface te1/0/1 vlan 2
Relay agent Information option is Enabled
Numeric Token format: hex
Circuit-id payload template: aaa$int-name$bbb$vlan-name-32$ccc
Remote-id payload template: aaa$switch-hostname-58$bbb
Total sub Options reserved payload: 137/247 bytes
Interface te1/0/1 vlan 2:
Error - Cannot calculate Circuit-ID info - sub-option contains VLAN related Token which
does not exist on device.
```



CHAPTER 14

DHCP Server Commands

This chapter contains the following sections:

- address (DHCP Host), on page 248
- address (DHCP Network), on page 249
- auto-default-router, on page 249
- bootfile, on page 250
- clear ip dhcp binding, on page 251
- client-name, on page 251
- default-router, on page 252
- dns-server, on page 253
- domain-name, on page 254
- ip dhcp excluded-address, on page 254
- ip dhcp pool host, on page 255
- ip dhcp pool network, on page 256
- ip dhcp server, on page 256
- lease, on page 257
- netbios-name-server, on page 258
- netbios-node-type, on page 258
- next-server, on page 259
- next-server-name, on page 260
- option , on page 261
- show ip dhcp, on page 262
- show ip dhcp allocated, on page 262
- show ip dhcp binding, on page 263
- show ip dhcp declined, on page 265
- show ip dhcp excluded-addresses, on page 265
- show ip dhcp expired, on page 266
- show ip dhcp pool host, on page 266
- show ip dhcp pool network, on page 267
- show ip dhcp pre-allocated, on page 268
- show ip dhcp server statistics, on page 269
- time-server, on page 269

address (DHCP Host)

To manually bind an IP address to a DHCP client, use the **address** command in DHCP Pool Host Configuration mode. To remove the IP address binding to the client, use the **no** form of this command.

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.
- ***mac-address***—Specifies the client MAC address.

Default Configuration

No address are bound.

Command Mode

DHCP Pool Host Configuration mode

User Guidelines

To classify the DHCP client, DHCP server uses either the client identifier passed in Option 61, if the **client-identifier** keyword is configured or the client MAC address, if the **hardware-address** keyword is configured.

Example

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

```
switchxxxxxx(config)# ip dhcp pool host aaaa
switchxxxxxx(config-dhcp)# address 10.12.1.99 255.255.255.0 client-identifier
01b7.0813.8811.66
switchxxxxxx(config-dhcp)# exit
switchxxxxxx(config)# ip dhcp pool host bbbb
switchxxxxxx(config-dhcp)# address 10.12.1.88 255.255.255.0 hardware-address 00:01:b7:08:13:88
switchxxxxxx(config-dhcp)# exit
switchxxxxxx(config)#
```

address (DHCP Network)

To configure the subnet number and mask for a DHCP address pool on a DHCP server, use the **address** command in DHCP Pool Network Configuration mode. To remove the subnet number and mask, use the **no** form of this command.

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.

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

auto-default-router

To enable auto default router, use the **auto-default-router** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To disable auto default router, use the **no** form of this command.

Syntax

auto-default-router

no auto-default-router

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

Enabled.

User Guidelines

If the feature is enabled then the DHCP server returns an IP address defined on the input interface as a default router when an default router is not configured in the following case:

- Default router is not configurable.
- DHCP client is directly connected.
- IP Routing is enabled.
- Default router was required by the client.

Example

The following example disable auto default router sending.

```
switchxxxxxx(config-dhcp)# no auto-default-router
```

bootfile

To specify the default boot image file name for a DHCP client, use the **bootfile** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To delete the boot image file name, use the **no** form of this command.

Syntax

bootfile *filename*

no bootfile

Parameters

- ***filename***—Specifies the file name used as a boot image. (Length: 1–128 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Example

The following example specifies boot_image_file as the default boot image file name for a DHCP client.

```
switchxxxxxx(config-dhcp)# bootfile boot_image_file
```

clear ip dhcp binding

To delete the dynamic address binding from the DHCP server database, use the **clear ip dhcp binding** command in Privileged EXEC mode.

Syntax

clear ip dhcp binding {*address* | *****}

Parameters

- ***address*** —Specifies the binding address to delete from the DHCP database.
- ***** —Clears all dynamic 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:

```
switchxxxxxx# clear ip dhcp binding 10.12.1.99
```

client-name

To define the name of a DHCP client, use the **client-name** command in DHCP Pool Host Configuration mode. To remove the client name, use the **no** form of this command.

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.

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

default-router

To configure the default router list for a DHCP client, use the **default-router** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the default router list, use the **no** form of this command.

Syntax

default-router *ip-address* [*ip-address2 ... ip-address8*]

no default-router

Parameters

- ***ip-address*** [*ip-address2 ... ip-address8*]—Specifies the IP addresses of default routers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host 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.

If the auto-default-router command is configured then the DHCP server returns an IP address defined on the input interface as a default router when an default router is not configured in the following case:

- Default router is not configurable.
- DHCP client is directly connected.
- IP Routing is enabled.
- Default router was required by the client.

Example

The following example specifies 10.12.1.99 as the default router IP address.

```
switchxxxxxx(config-dhcp)# default-router 10.12.1.99
```

dns-server

To configure the Domain Name System (DNS) IP server list available to a DHCP client, use the **dns-server** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the DNS server list, use the **no** form of this command.

Syntax

dns-server *ip-address* [*ip-address2 ... ip-address8*]

no dns-server

Parameters

- ***ip-address*** [*ip-address2 ... ip-address8*]—Specifies the IP addresses of DNS servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host 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.

```
switchxxxxxx(config-dhcp)# dns-server 10.12.1.99
```

domain-name

To specify the domain name for a DHCP client, use the **domain-name** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the domain name, use the **no** form of this command.

Syntax

domain-name *domain*

no domain-name

Parameters

- ***domain***—Specifies the DHCP client domain name string. (Length: 1–32 characters).

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No domain name is defined.

Example

The following example specifies yahoo.com as the DHCP client domain name string.

```
switchxxxxxx(config-dhcp)# domain-name yahoo.com
```

ip dhcp excluded-address

To specify IP addresses that a DHCP server must not assign to DHCP clients, use the **ip dhcp excluded-address** command in Global Configuration mode. To remove the excluded IP addresses, use the **no** form of this command.

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***—(Optional) 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.

```
switchxxxxxx(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

ip dhcp pool host

To configure a DHCP static address on a DHCP server and enter the DHCP Pool Host Configuration mode, use the **ip dhcp pool host** command in Global Configuration mode. To remove the address pool, use the **no** form of this command.

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. 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:

```
switchxxxxxx(config)# ip dhcp pool host station
switchxxxxxx(config-dhcp)#
```

ip dhcp pool network

To configure a DHCP address pool on a DHCP Server and enter DHCP Pool Network Configuration mode, use the **ip dhcp pool network** command in Global Configuration mode. To remove the address pool, use the **no** form of this command.

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. 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.

```
switchxxxxxx(config)# ip dhcp pool network Pool1
switchxxxxxx(config-dhcp)#
```

ip dhcp server

To enable the DHCP server features on the device, use the **ip dhcp server** command in Global Configuration mode. To disable the DHCP server, use the **no** form of this command.

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:

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

lease

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 **lease** command in DHCP Pool Network Configuration mode. To restore the default value, use the **no** form of this command.

Syntax

lease *days* [*hours* [*minutes*]] | **infinite**

no lease

Parameters

- ***days***—Specifies the number of days in the lease.
- ***hours***—(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before configuring an *hours* value.
- ***minutes***—(Optional) 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.

```
switchxxxxxx(config-dhcp)# lease 1
```

The following example shows a one-hour lease.

```
switchxxxxxx(config-dhcp)# lease 0 1
```

The following example shows a one-minute lease.

```
switchxxxxxx(config-dhcp)# lease 0 0 1
```

The following example shows an infinite (unlimited) lease.

```
switchxxxxxx(config-dhcp)# lease infinite
```

netbios-name-server

To configure the NetBIOS Windows Internet Naming Service (WINS) server list that is available to Microsoft DHCP clients, use the **netbios-name-server** in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the NetBIOS name server list, use the **no** form of this command.

Syntax

netbios-name-server *ip-address* [*ip-address2 ... ip-address8*]

no netbios-name-server

Parameters

- ***ip-address*** [***ip-address2*** ... ***ip-address8***]—Specifies the IP addresses of NetBIOS WINS name servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host 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.

```
switchxxxxxx(config-dhcp)# netbios-name-server 10.12.1.90
```

netbios-node-type

To configure the NetBIOS node type for Microsoft DHCP clients, use the **netbios-node-type** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To return to default, use the **no** form of this command.

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 Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

h-node (Hybrid NetBIOS node type).

Example

The following example specifies the client's NetBIOS type as mixed.

```
switchxxxxxx(config-dhcp)# netbios node-type m-node
```

next-server

To configure the next server (siaddr) in the boot process of a DHCP client, use the **next-server** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the next server, use the **no** form of this command.

Syntax

next-server *ip-address*

no next-server

Parameters

- ***ip-address***—Specifies the IP address of the next server in the boot process.

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 Network Configuration mode

DHCP Pool Host Configuration mode

User Guidelines

The client will connect, using the SCP/TFTP protocol, to this server in order to download the configuration file.

Example

The following example specifies 10.12.1.99 as the IP address of the next server:

```
switchxxxxxx(config-dhcp)# next-server 10.12.1.99
```

next-server-name

To configure the next server name (sname) in the boot process of a DHCP client, use the **next-server-name** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the boot server name, use the **no** form of this command.

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 Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No next server name is defined.

User Guidelines

The client will connect, using the SCP/TFTP protocol, to this server in order to download the configuration file.

Example

The following example specifies www.bootserver.com as the name of the next server in the boot process of a DHCP client.

```
switchxxxxxx(config-dhcp)# next-server www.bootserver.com
```

option

To configure the DHCP server options, use the **option** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the options, use the **no** form of this command.

Syntax

option *code* {**boolean** {**false** | **true**} | **integer** *value* | **ascii** *string* | **hex** {*string* | **none**} | **ip** {*address*} | **ip-list** {*ip-address1* [*ip-address2* …]}} [**description** *text*]

no option *code*

Parameters

- ***code***—Specifies the DHCP option code. The supported values are defined in the User Guidelines.
- **boolean** {**false** | **true**}—Specifies a boolean value. The values are coded by integer values of one octet: 0 = false and 1 = true.
- **integer** *value*—Specifies an integer value. The option size depends on the option code.
- **ascii** *string*—Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white spaces must be delimited by quotation marks. The ASCII value is truncated to the first 160 characters entered.
- **ip** *address*—Specifies an IP address.
- **ip-list** {*ip-address1* [*ip-address2* ...]}—Specifies up to 8 IP addresses.
- **hex** *string*—Specifies dotted hexadecimal data. The hexadecimal value is truncated to the first 320 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.
- **hex none**—Specifies the zero-length hexadecimal string.
- **description** *text*—User description

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

User Guidelines

The **option** command enables defining any option that cannot be defined by other special CLI commands. A new definition of an option overrides the previous definition of this option.

The **boolean** keyword may be configured for the following options: 19, 20, 27, 29-31, 34, 36, and 39.

The **integer** keyword may be configured for the following options: 2, 13, 22-26, 35, 37-38, 132-134, and 211. The switch checks the value range and builds the value field of the size in accordance with the **option** definition.

The **ascii** keyword may be configured for the following options: 14, 17-18, 40, 64, 130, 209, and 210.

The **ip** keyword may be configured for the following options: 16, 28, 32, 128-129, 131, 135, and 136.

The **ip-list** keyword may be configured for the following options: 5, 7-11, 33, 41, 42, 45, 48, 49, 65, 68-76, and 150.

The **hex** keyword may be configured for any option in the range 1-254 except for the following: 1, 3-4, 6, 12, 15, 44, 46, 50-51, 53-54, 56, 66-67, 82, and 255. The switch does not validate the syntax of an option defined by this format.

Example 1. The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding:

```
switchxxxxxx(config-dhcp)# option 19 boolean true description "IP Forwarding Enable/Disable
 Option"
```

Example 2. The following example configures DHCP option 2, which specifies the offset of the client in seconds from Coordinated Universal Time (UTC):

```
switchxxxxxx(config-dhcp)# option 2 integer 3600
```

Example 3. 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:

```
switchxxxxxx(config-dhcp)# option 72 ip-list 172.16.3.252 172.16.3.253
```

show ip dhcp

To display the DHCP configuration, use the **show ip dhcp** command in User EXEC mode.

Syntax

show ip dhcp

Command Mode

User EXEC mode

Example

The following example displays the DHCP configuration.

```
switchxxxxxx# show ip dhcp
DHCP server is enabled.
```

show ip dhcp allocated

To display the allocated address or all the allocated addresses on the DHCP server, use the **show ip dhcp allocated** command in User EXEC mode.

Syntax

show ip dhcp allocated [*ip-address*]

Parameters

- ***ip-address*** —(Optional) Specifies the IP address.

Command Mode

User EXEC mode

Example

The following example displays the output of various forms of this command:

```
switchxxxxxx# 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
switchxxxxxx# 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
switchxxxxxx# 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.

show ip dhcp binding

To display the specific address binding or all the address bindings on the DHCP server, use the **show ip dhcp binding** command in User EXEC mode.

Syntax

show ip dhcp binding [***ip-address***]

Parameters

- ***ip-address***—(Optional) Specifies the IP address.

Command Mode

User EXEC mode

Examples

The following examples display the DHCP server binding address parameters.

```
switchxxxxxx# 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 Client Identifier  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
switchxxxxxx# show ip dhcp binding 1.16.1.11
DHCP server enabled
IP address Client Identifier  Lease Expiration  Type    State
---------- -----------------  ----------------- ------- ---------
1.16.1.11  00a0.9802.32de     Feb 01 1998      dynamic allocated
                              12:00 AM
switchxxxxxx# show ip dhcp binding 1.16.3.24
IP address Client Identifier   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.
Client Identifier	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.

show ip dhcp declined

To display the specific declined address or all of the declined addresses on the DHCP server, use the **show ip dhcp declined** command in User EXEC mode.

Syntax

show ip dhcp declined [*ip-address*]

Parameters

- ***ip-address***—(Optional) Specifies the IP address.

Command Mode

User EXEC mode

Example

The following example displays the output of various forms of this command:

```
switchxxxxxx# 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
switchxxxxxx# 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
```

show ip dhcp excluded-addresses

To display the excluded addresses, use the **show ip dhcp excluded-addresses** command in User EXEC mode.

Syntax

show ip dhcp excluded-addresses

Command Mode

User EXEC mode

Example

The following example displays excluded addresses.

```
switchxxxxxx# 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
```

show ip dhcp expired

To display the specific expired address or all of the expired addresses on the DHCP server, use the **show ip dhcp expired** command in User EXEC mode.

Syntax

show ip dhcp expired [*ip-address*]

Parameters

- ***ip-address***—(Optional) Specifies the IP.

Command Mode

User EXEC mode

Example

```
switchxxxxxx# 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
switchxxxxxx# 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
```

show ip dhcp pool host

To display the DHCP pool host configuration, use the **show ip dhcp pool host** command in User EXEC mode.

Syntax

show ip dhcp pool host [*address* | *name*]

Parameters

- ***address***—(Optional) Specifies the client IP address.
- ***name***—(Optional) Specifies the DHCP pool name. (Length: 1-32 characters)

Command Mode

User EXEC mode

Example 1. The following example displays the configuration of all DHCP host pools:

```
switchxxxxxx# 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 of the pool named **station**:

```
switchxxxxxx# 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
Auto Default router: enabled
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 Type     Len Value             Description
---  -------  --- ----------------  --------------------------------
2    integer    4 3600
14   ascii     16 qq/aaaa/bbb.txt
19   boolean    1 false                "IP Forwarding Enable/Disable
                                         Option"
21   ip         4 134.14.14.1
31   ip-list    8 1.1.1.1, 12.23.45.2
47   hex        5 02af00aa00
```

show ip dhcp pool network

To display the DHCP network configuration, use the **show ip dhcp pool network** command in User EXEC mode.

Syntax

show ip dhcp pool network [*name*]

Parameters

- ***name***—(Optional) Specifies the DHCP pool name. (Length: 1-32 characters).

Command Mode

User EXEC mode

Example 1—The following example displays configuration of all DHCP network pools:

```
switchxxxxxx# 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
```

Example 2—The following example displays configuration of the DHCP network pool **marketing**:

```
switchxxxxxx# 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
Auto Default router: enabled
Default router: 10.1.1.1
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 Type     Len Value                 Description
---  -------  --- --------------------  --------------------------------
2    integer    4 3600
14   ascii     16 qq/aaaa/bbb.txt
19   boolean    1 false                 "IP Forwarding Enable/Disable
                                          Option"
21   ip         4 134.14.14.1
31   ip-list    8 1.1.1.1, 12.23.45.2
47   hex        5 02af00aa00
```

show ip dhcp pre-allocated

To display the specific pre-allocated address or all the pre-allocated addresses on the DHCP server, use the **show ip dhcp pre-allocated** command in User EXEC mode.

Syntax

show ip dhcp pre-allocated [*ip-address*]

Parameters

- ***ip-address***—(Optional) Specifies the IP.

Command Mode

User EXEC mode

Examples

```
switchxxxxxx# 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
switchxxxxxx# 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
```

show ip dhcp server statistics

To display DHCP server statistics, use the **show ip dhcp server statistics** command in User EXEC mode.

Syntax

show ip dhcp server statistics

Command Mode

User EXEC mode

Example

The following example displays DHCP server statistics

```
switchxxxxxx# show ip 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
```

time-server

To specify the time servers list for a DHCP client, use the **time-server** command in DHCP Pool Network Configuration mode or in DHCP Pool Host Configuration mode. To remove the time servers list, use the **no** form of this command.

Syntax

time-server *ip-address* [*ip-address2 ... ip-address8*]

no time-server

Parameters

- ***ip-address*** [*ip-address2 ... ip-address8*]—Specifies the IP addresses of Time servers. Up to eight addresses can be specified in one command line.

Command Mode

DHCP Pool Network Configuration mode

DHCP Pool Host Configuration mode

Default Configuration

No time server is defined.

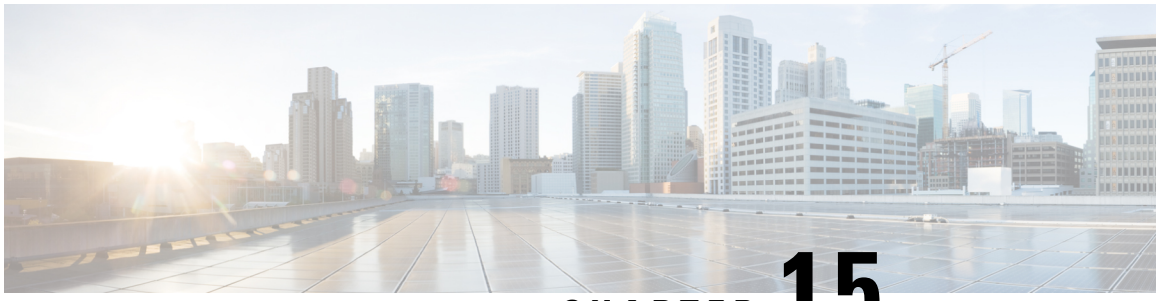
User Guidelines

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.

```
switchxxxxxx(config-dhcp)# time-server 10.12.1.99
```



CHAPTER 15

DHCP Snooping Commands

This chapter contains the following sections:

- ip dhcp snooping, on page 272
- ip dhcp snooping vlan, on page 272
- ip dhcp snooping trust, on page 273
- ip dhcp snooping information option allowed-untrusted, on page 273
- ip dhcp snooping verify, on page 274
- ip dhcp snooping database, on page 274
- ip dhcp snooping binding, on page 275
- clear ip dhcp snooping database, on page 276
- show ip dhcp snooping, on page 276
- show ip dhcp snooping binding, on page 277
- ip source-guard, on page 278
- ip source-guard binding, on page 279
- ip source-guard tcam retries-freq, on page 279
- ip source-guard tcam locate, on page 280
- show ip source-guard configuration, on page 281
- show ip source-guard status, on page 281
- show ip source-guard inactive, on page 282
- show ip source-guard statistics, on page 283
- ip arp inspection, on page 283
- ip arp inspection vlan, on page 284
- ip arp inspection trust, on page 284
- ip arp inspection validate, on page 285
- ip arp inspection list create, on page 286
- ip mac, on page 286
- ip arp inspection list assign, on page 287
- ip arp inspection logging interval, on page 288
- show ip arp inspection, on page 288
- show ip arp inspection list, on page 289
- show ip arp inspection statistics, on page 289
- clear ip arp inspection statistics, on page 290

ip dhcp snooping

Use the **ip dhcp snooping** Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping

no ip dhcp snooping

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled.

Example

The following example enables DHCP Snooping on the device.

```
switchxxxxxx(config)# ip dhcp snooping
```

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 *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.

```
switchxxxxxx(config)# ip dhcp snooping vlan 21
```

ip dhcp snooping trust

Use the **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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 gi1/0/4 as trusted for DHCP Snooping.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# ip dhcp snooping trust
```

ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the **no** form of this command to drop these packets from an untrusted port.

Syntax

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Default Configuration

DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode

Global Configuration mode

Example

The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
switchxxxxxx(config)# ip dhcp snooping information option allowed-untrusted
```

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.

```
switchxxxxxx(config)# ip dhcp snooping verify
```

ip dhcp snooping database

Use the **ip dhcp snooping database** Global Configuration mode command to enable the DHCP Snooping binding database file. Use the **no** form of this command to delete the DHCP Snooping binding database file.

Syntax

ip dhcp snooping database

no ip dhcp snooping database

Default Configuration

The DHCP Snooping binding database file is not defined.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Snooping binding database file resides on Flash. To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured. The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example

The following example enables the DHCP Snooping binding database file.

```
switchxxxxxx(config)# ip dhcp snooping database
```

ip dhcp snooping binding

Use the **ip dhcp snooping binding** Privileged EXEC mode command to configure the DHCP Snooping binding database and add dynamic 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: 10–4294967294).
  - **infinite**—Specifies infinite lease time.

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **ip dhcp snooping binding** command to add manually a dynamic entry to the DHCP database.

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 would not be added to the configuration files. The entry would be displayed in the show commands as a “DHCP Snooping” entry. An entry added by this command can override the existed dynamic entry. The entry is displayed in the show commands as a DHCP Snooping entry.

Use the **no ip dhcp snooping binding** command to delete manually a dynamic entry from the DHCP database.

A dynamic temporary entries for which the IP address is 0.0.0.0 cannot be deleted.

Example

The following example adds a binding entry to the DHCP Snooping binding database.

```
switchxxxxxx# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 gi1/0/4 expiry 900
```

clear ip dhcp snooping database

Use the **clear ip dhcp snooping database** Privileged EXEC mode command to clear the DHCP Snooping binding database.

Syntax

clear ip dhcp snooping database

Command Mode

Privileged EXEC mode

Example

The following example clears the DHCP Snooping binding database.

```
switchxxxxxx# clear ip dhcp snooping database
```

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

User EXEC mode

Example

The following example displays the DHCP snooping configuration.

```
switchxxxxxx# 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
---	---
gi1/0/1	Yes
gi1/0/2	Yes

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.-

```
switchxxxxxx# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 2
```

Mac Address	IP Address	Lease (sec)	Type	VLAN	Interface
0060.704C.73FF	10.1.8.1	7983	snooping	3	gi1/0/1
0060.704C.7BC1	10.1.8.2	92332	snooping (s)	3	gi1/0/2

ip source-guard

Use the **ip source-guard** command in Configuration mode or Interface 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

Default Configuration

IP Source Guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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 gi1/0/4.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# ip source-guard
```

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

Use the **ip source-guard binding** command to add a static entry to the DHCP database.

An entry added by this command can override the existed entry.

Use the **no ip source-guard binding** command to delete an entry from the DHCP database.

Example

The following example configures the static IP source bindings.

```
switchxxxxxx(config)# ip source-guard binding 0060.704C.73FF 23 176.10.1.1 gi1/0/4
```

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.

Example

The following example sets the frequency of retries for TCAM resources to 2 minutes.

```
switchxxxxxx(config)# ip source-guard tcam retries-freq 120
```

ip source-guard tcam locate

Use the **ip source-guard tcam locate** Privileged EXEC mode command to manually retry to locate TCAM resources for inactive IP Source Guard addresses.

Syntax

ip source-guard tcam locate

Command Mode

Privileged EXEC mode

User Guidelines

Since the IP Source Guard uses the Ternary Content Addressable Memory (TCAM) resources, there may be situations when IP Source Guard addresses are inactive because of a lack of TCAM resources.

By default, once every 60 seconds the software conducts a search for available space in the TCAM for the inactive IP Source Guard addresses.

Example

The following example manually retries to locate TCAM resources.

```
switchxxxxxx# ip source-guard tcam locate
```

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

User EXEC mode

Example

The following example displays the IP Source Guard configuration.

```
switchxxxxxx# show ip source-guard configuration
IP source guard is globally enabled.

Interface                       State
---------                       -------
gi1/0/1                         Enabled
gi1/0/2                         Enabled
gi1/0/3                         Enabled
gi1/0/4                         Enabled
```

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

User EXEC mode

Example

The following examples display the IP Source Guard status.

```
switchxxxxxx# show ip source-guard status
IP source guard is globally enaabled.

Interface   Filter   Status     IP Address    MAC Address          VLAN   Type
---------   ------   --------   -----------   ------------------   ----   ------
gi1/0/1     IP       Active     10.1.8.1      0060.704C.73FF       3      DHCP
gi1/0/2     IP       Active     10.1.8.2      0060.704C.7BC1       3      Static
gi1/0/3     IP       Active     Deny all      0060.704C.7BC3       4      DHCP
gi1/0/4     IP       Inactive
```

show ip source-guard inactive

Use the **show ip source-guard inactive** EXEC mode command to display the IP Source Guard inactive addresses.

Syntax

show ip source-guard inactive

Command Mode

User 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.

Example

The following example displays the IP source guard inactive addresses.

```
switchxxxxxx# show ip source-guard inactive
TCAM resources search frequency: 60 seconds
```

Interface	Filter	IP Address	MAC Address	VLAN	Type	Reason
gi1/0/2	IP	10.1.8.32	0060.704C.83FF	3	DHCP	Resource
gi1/0/3	IP					Problem
gi1/0/4	I					Trust port

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

User EXEC mode

Example

switchxxxxxx# show ip source-guard statistics

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

ip arp inspection

Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

Syntax

ip arp inspection

no ip arp inspection

Default Configuration

ARP inspection is disabled.

Command Mode

Global Configuration mode

User Guidelines

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

Example

The following example enables ARP inspection on the device.

```
switchxxxxxx(config)# ip arp inspection
```

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.

Example

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
switchxxxxxx(config)# ip arp inspection vlan 23
```

ip arp inspection trust

Use the **ip arp inspection trust** Interface Configuration (Ethernet, Port-channel) mode command to configure an interface trust state that determines if incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection trust

no ip arp inspection trust

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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.

Example

The following example configures gi1/0/3 as a trusted interface.

```
switchxxxxxx(config)# interface gi1/0/3
switchxxxxxx(config-if)# ip arp inspection trust
```

ip arp inspection validate

Use the **ip arp inspection validate** Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection validate

no ip arp inspection validate

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address**: Compares the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.

- **Destination MAC address**: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- **IP addresses**: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

```
switchxxxxxx(config)# ip arp inspection validate
```

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.

```
switchxxxxxx(config)# ip arp inspection list create servers
```

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.

```
switchxxxxxx(config)# ip arp inspection list create servers
switchxxxxxx(config-arp-list)# ip 172.16.1.1 mac 0060.704C.7321
switchxxxxxx(config-arp-list)# ip 172.16.1.2 mac 0060.704C.7322
```

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.

```
switchxxxxxx(config)# ip arp inspection list assign 37 servers
```

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.

```
switchxxxxxx(config)# ip arp inspection logging interval 60
```

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

User EXEC mode

Example

The following example displays the ARP inspection configuration.

```
switchxxxxxx# 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
----------- -----------
gi1/0/1          Yes
gi1/0/2          Yes
```

show ip arp inspection list

Use the **show ip arp inspection list** Privileged EXEC mode command to display the static ARP binding list.

Syntax

show ip arp inspection list

Command Mode

Privileged EXEC mode

Example

The following example displays the static ARP binding list.

```
switchxxxxxx# 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

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

User EXEC mode

User Guidelines

Counters values are kept when disabling the ARP Inspection feature.

Example

```
switchxxxxxx# show ip arp inspection statistics
Vlan   Forwarded Packets Dropped Packets   IP/MAC Failures
----  ----------------- ---------------  ---------------
2     1500           100                        80
```

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

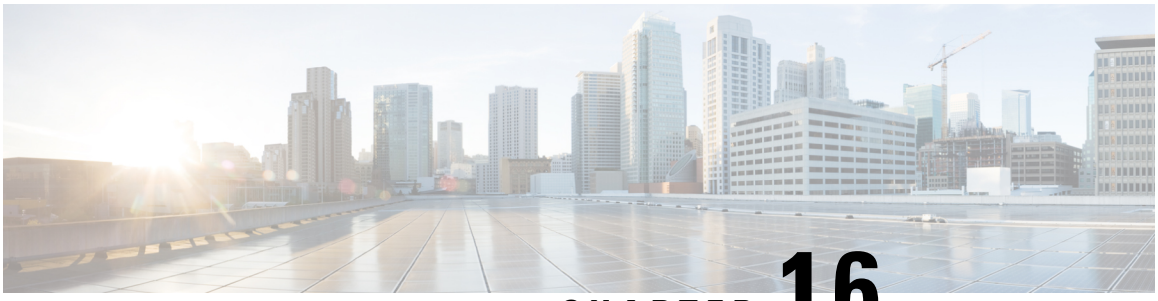
- ***vlan-id***—Specifies VLAN ID.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip arp inspection statistics
```



CHAPTER 16

DHCPv6 Commands

This chapter contains the following sections:

- clear ipv6 dhcp client, on page 291
- ipv6 address dhcp, on page 292
- ipv6 dhcp client information refresh, on page 294
- ipv6 dhcp client information refresh minimum, on page 295
- ipv6 dhcp duid-en, on page 296
- ipv6 dhcp relay destination (Global), on page 297
- ipv6 dhcp relay destination (Interface), on page 298
- show ipv6 dhcp, on page 300
- show ipv6 dhcp interface, on page 301

clear ipv6 dhcp client

To restart DHCP for an IPv6 client on an interface, use the **clear ipv6 dhcp client** command in Privileged EXEC mode.

Syntax

clear ipv6 dhcp client *interface-id*

Parameters

- ***interface-id***—Interface identifier.

Command Mode

Privileged EXEC mode

User Guidelines

This command restarts DHCP for an IPv6 client on a specified interface after first releasing and unconfiguring previously-acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Example

The following example restarts the DHCP for IPv6 client on VLAN 100:

```
switchxxxxxx# clear ipv6 dhcp client vlan 100
```

ipv6 address dhcp

To enable DHCP for an IPv6 client process and acquire an IPv6 address on an interface, use the **ipv6 address dhcp** command in Interface Configuration mode. To remove the address from the interface, use the **no** form of this command.

Syntax

ipv6 address dhcp [**rapid-commit**]

no ipv6 address dhcp

Parameters

- **rapid-commit**—Allows the two-message exchange method for address assignment.

Default Configuration

No IPv6 addresses are acquired from the DHCPv6 server.

Command Mode

Interface (VLAN) Configuration mode

Interface (Ethernet, Port Channel, OOB) Configuration mode

User Guidelines

This command enables IPv6 on an interface (if it is not enabled) and starts the DHCP for IPv6 client process, if this process is not yet running and if an IPv6 interface is enabled on the interface. This command allows an interface to dynamically learn its IPv6 address by using DHCPv6 and enables the DHCPv6 Stateless service.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

This command allows an interface to dynamically learn its IPv6 address by using DHCPv6.

The DHCPv6 stateless service allows to receive the configuration from a DHCP server, passed in the following options:

- Option 7: OPTION_PREFERENCE - The preference value for the server in this message
- Option 12: OPTION_UNICAST - The IP address to which the client should send messages delivered using unicast
- Option 23: OPTION_DNS_SERVERS - List of DNS Servers IPv6 Addresses
- Option 24: OPTION_DOMAIN_LIST - Domain Search List
- Option 31: OPTION_SNTP_SERVERS - List of SNTP Servers IPv6 Addresses

- Option 32: OPTION_INFORMATION_REFRESH_TIME - Information Refresh Time Option
- Option 41: OPTION_NEW_POSIX_TIMEZONE - New Timezone Posix String
- Option 59: OPT_BOOTFILE_URL - Configuration Server URL

  Option 60: OPT_BOOTFILE_PARAM, the first parameter - Configuration File Path Name

The DHCPv6 client uses the following IAID format based on the interface-id on which it is running:

- Octet 1, bits 7-4: These bits are reserved and must be 0
- Octet 1, Bits 3-0: These bits contain the interface type:

  0—VLAN
  - 1—Ethernet port
  - 2—Port channel
  - 3—Tunnel
- Octets 2-4: The octets contain a value depending on the interface type in the network format:
  - VLAN

Octet 2: Reserved, must be 0

Octets 3-4: VLAN ID (1-4095)

- Ethernet port

Octet 2, bits 7-4: Slot number

Octet 2, bits 3-0: Port Type:

0—Ethernet

1—Fast Ethernet

2—Giga Ethernet

3—2.5 Giga Ethernet

4—5 Giga Ethernet

5—10 Giga Ethernet

6—12 Giga Ethernet

7—13.6 Giga Ethernet

8—16 Giga Ethernet

9—20 Giga Ethernet

10—40 Giga Ethernet

11—100 Giga Ethernet

Octet 3: Unit number

Octet 4: Port number

- Port channel

Octets 2-3: Reserved, must be 0

Octet 4: Port channel number

- Tunnel

Octets 2-3: Reserved, must be 0

Octet 4: Tunnel number

When IPv6 Forwarding is enabled only stateless information is required from a DHCPv6 server.

When IPv6 forwarding is changed from disabled to enabled, IPv6 addresses assigned by a DHCPv6 are removed.

When IPv6 forwarding is changed from enabled to disabled receiving IPv6 addresses from a DHCPv6 server is resumed.

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface.

Example

The following example enables IPv6 on VLAN 100 and acquires an IPv6 address:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address dhcp
switchxxxxxx(config-if)# exit
```

ipv6 dhcp client information refresh

To configure the refresh time for IPv6 client information refresh time on a specified interface if the DHCPv6 server reply does not include the Information Refresh Time, use the **ipv6 dhcp client information refresh** command in Interface Configuration mode. To return to the default value of the refresh time, use the **no** form of this command.

Syntax

ipv6 dhcp client information refresh *seconds* | **infinite**

no ipv6 dhcp client information refresh

Parameters

- ***seconds***—The refresh time, in seconds. The value cannot be less than the minimal acceptable refresh time configured by the **ipv6 dhcp client information refresh** command. The maximum value that can be used is 4,294967,294 seconds (0xFFFFFFFE).
- **infinite**—Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface Configuration mode

User Guidelines

The **ipv6 dhcp client information refresh** command specifies the information refresh time. If the server does not sends an information refresh time option then a value configured by the command is used.

Use the **infinite** keyword, to prevent refresh, if the server does not send an information refresh time option.

Example

The following example configures an upper limit of 2 days:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp client information refresh 172800
switchxxxxxx(config-if)# exit
```

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable refresh time on the specified interface, use the **ipv6 dhcp client information refresh minimum** command in Interface Configuration mode. To remove the configured refresh time, use the **no** form of this command.

Syntax

ipv6 dhcp client information refresh minimum *seconds* | **infinite**

no ipv6 dhcp client information refresh minimum

Parameters

- ***seconds***—The refresh time, in seconds. The minimum value that can be used is 600 seconds. The maximum value that can be used is 4,294,967,294 seconds (0xFFFFFFFE).
- **infinite**—Infinite refresh time.

Default Configuration

The default is 86,400 seconds (24 hours).

Command Mode

Interface Configuration mode

User Guidelines

The **ipv6 dhcp client information refresh minimum** command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in the following situations:

- In unstable environments where unexpected changes are likely to occur.

- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

If you configure the **infinite** keyword client never refreshes the information.

Example

The following example configures an upper limit of 2 days:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp client information refresh 172800
switchxxxxxx(config-if)# exit
```

ipv6 dhcp duid-en

To set the Vendor Based on Enterprise Number DHVPv6 Unique Identified (DUID-EN) format, use the **ipv6 dhcp duid-en** command in Global Configuration mode.

To return to the default value, use the **no** form of this command.

Syntax

ipv6 dhcp duid-en *enterprise-number identifier*

no ipv6 dhcp duid-en

Parameters

- ***enterprise-number***—The vendor's registered Private Enterprise number as maintained by IANA.
- ***identifier***—The vendor-defined non-empty hex string (up to 64 hex characters). If the number of the character is not even '0' is added at the right. Each 2 hex characters can be separated by a period or colon.

Default Configuration

DUID Based on Link-layer Address (DUID-LL) is used. The base MAC Address is used as a Link-layer Address.

Command Mode

Global Configuration mode

User Guidelines

By default, the DHCPv6 uses the DUID Based on Link-layer Address (see RFC3315) with the Base MAC Address as a Link-layer Address.

Use this command to change the DUID format to the Vendor Based on Enterprise Number.

Example 1. The following sets the DIID-EN format:

```
ipv6 dhcp duid-en 9 0CC084D303000912
```

Example 2. The following sets the DIID-EN format using colons as delimiter:

```
switchxxxxxx(config)# ipv6 dhcp duid-en 9 0C:C0:84:D3:03:00:09:12
```

ipv6 dhcp relay destination (Global)

To specify a globally-defined relay destination address to which client messages are forwarded, use the **ipv6 dhcp relay destination** command in Global Configuration mode. To remove a relay destination address, use the **no** form of this command.

Syntax

ipv6 dhcp relay destination {*ipv6-address* [*interface-id*]} | *interface-id*

no ipv6 dhcp relay destination [{*ipv6-address* [*interface-id*]} | *interface-id*]

Parameters

- ***ipv6-address*** [*interface-id*]—Relay destination IPv6 address in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons. There are the following types of relay destination address:
  - Link-local Unicast address. A user must specify the *interface-id* argument for this kind of address
  - Global Unicast IPv6 address. If the *interface-id* argument is omitted then the Routing table is used.
- ***interface-id***—Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the well-known link-local Multicast address **All_DHCP_Relay_Agents_and_Servers** (FF02::1:2) through the link to which the output interface is connected.

Default Configuration

There is no globally-defined relay destination.

Command Mode

Global Configuration mode

User Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded. The address is used by all DHCPv6 relays running on the switch. Up to 100 addresses can be defined.

When a relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per interface and globally. Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. Unspecified, loopback, and Multicast addresses are not acceptable as the relay destination.

Use the **no** form of the command with the *ipv6-address* and *interface-id* arguments to remove only the given globally-defined address with the given output interface.

Use the **no** form of the command with the *ipv6-address* argument to remove only the given globally-defined address for all output interfaces.

The **no** form of the command without the arguments removes all the globally-defined addresses.

Example 1. The following example sets the relay unicast link-local destination address per VLAN 200:

```
switchxxxxxx(config)# ipv6 dhcp relay destination FE80::1:2 vlan 200
```

Example 2. The following example sets that client messages are forwarded to VLAN 200:

```
switchxxxxxx(config)# ipv6 dhcp relay destination vlan 200
```

Example 3. The following example sets the unicast global relay destination address:

```
switchxxxxxx(config)# ipv6 dhcp relay destination 3002::1:2
```

ipv6 dhcp relay destination (Interface)

To specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in Interface Configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

Syntax

ipv6 dhcp relay destination [{*ipv6-address* [*interface-id*]} | *interface-id*]

no ipv6 dhcp relay destination [{*ipv6-address* [*interface-id*]} | *interface-id*]

Parameters

- ***ipv6-address*** [*interface-id*]—Relay destination IPv6 address in the form documented in RFC 4291 where the address is specified in hexadecimal using 16-bit values between colons. There are the following types of relay destination address:
  - Link-local Unicast address. A user must specify the *interface-id* argument for this kind of address
  - Global Unicast IPv6 address. If the *interface-id* argument is omitted then the Routing table is used.
- ***interface-id***—Interface identifier that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the well-known link-local Multicast address **All_DHCP_Relay_Agents_and_Servers** (FF02::1:2) through the link to which the output interface is connected.

Default Configuration

The relay function is disabled, and there is no relay destination on an interface.

Command Mode

Interface Configuration mode

User Guidelines

This command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. Up to 10 addresses can be defined per one interface and up to 100 addresses can be defined per switch.

DHCPv6 Relay inserts the Interface-id option if an IPv6 global address is not defined on the interface on which the relay is running. The Interface-id field of the option is the interface name (a value of the **ifName** field of the **ifTable**) on which the relay is running.

When relay service is running on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations configured per interface and globally.

The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a Unicast address of a server or another relay agent, or it may be a Multicast address. There are two types of relay destination addresses:

- A link-local Unicast or Multicast IPv6 address, for which a user must specify an output interface
- A global Unicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a Unicast or Multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a Multicast address, it sets the hop limit field in the IPv6 packet header to 32. Unspecified, loopback, and node-local Multicast addresses are not acceptable as the relay destination.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface.

Use the **no** form of the command with arguments to remove a specific address.

Use the **no** form of the command without arguments to remove all the defined addresses and to disable the relay on the interface.

Example 1. The following example sets the relay Unicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination FE80::1:2 vlan 200
switchxxxxxx(config-if)# exit
```

Example 2. The following example sets the relay well known Multicast link-local destination address per VLAN 200 and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination vlan 200
switchxxxxxx(config-if)# exit
```

Example 3. The following example sets the Unicast global relay destination address and enables the DHCPv6 Relay on VLAN 100 if it was not enabled:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination 3002::1:2
switchxxxxxx(config-if)# exit
```

Example 4. The following example enables DHCPv6 relay on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp relay destination
switchxxxxxx(config-if)# exit
```

Example 5. The following example disables DHCPv6 relay on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 dhcp relay destination
switchxxxxxx(config-if)# exit
```

show ipv6 dhcp

To display the Dynamic DHCP unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in User EXEC mode.This information is relevant for DHCPv6 clients and DHCPv6 relays.

Syntax

show ipv6 dhcp

Command Mode

User EXEC mode

User Guidelines

This command uses the DUID, which is based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID.

Example 1. The following is sample output from this command when the switch's DUID format is vendor based on enterprise number:

```
switchxxxxxx# show ipv6 dhcp
The switch's DHCPv6 unique identifier(DUID)is 0002000000090CC084D303000912
  Format: 2
  Enterprise Number: 9
  Identifier: 0CC084D303000912
```

Example 2. The following is sample output from this command when the switch's DUID format is the vendor-based on link-layer address:

```
switchxxxxxx# show ipv6 dhcp
The switch's DHCPv6 unique identifier(DUID)is 000300010024012607AA
  Format: 3
  Hardware type: 1
  MAC Address: 0024.0126.07AA
```

Example 3. The following is sample output from this command when the switch's DUID format is vendorbased on link-layer address and DHCPv6 Relay is supported:

```
switchxxxxxx# show ipv6 dhcp
The switch's DHCPv6 unique identifier(DUID)is 000300010024012607AA
  Format: 3
  Hardware type: 1
  MAC Address: 0024.0126.07AA
Relay Destinations:
  2001:001:250:A2FF:FEBF:A056
  2001:1001:250:A2FF:FEBF:A056
```

```
2001:1011:250:A2FF:FEBF:A056 via VLAN 100
FE80::250:A2FF:FEBF:A056 via VLAN 100
FE80::250:A2FF:FEBF:A056 via VLAN 200
```

show ipv6 dhcp interface

To display DHCP for IPv6 interface information, use the **show ipv6 dhcp interface** command in User EXEC mode.

Syntax

show ipv6 dhcp interface [*interface-id*]

Parameters

- ***interface-id***—Interface identifier.

Command Mode

User EXEC mode

User Guidelines

If no interfaces are specified in the command, all interfaces on which DHCP for IPv6 (client or server) is enabled are displayed. If an interface is specified in the command, only information about the specified interface is displayed.

Note. This new output format is supported starting with the SW version supporting statefull configuration

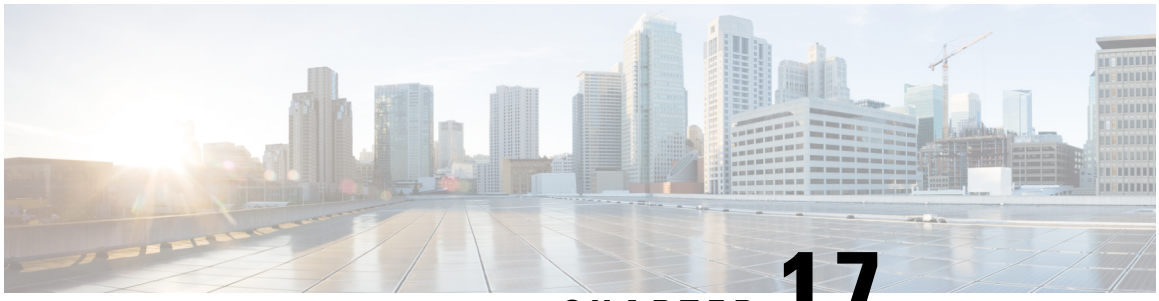
Example

The following is sample output from this command when DHCPv6 client is enabled:

```
switchxxxxxx# show ipv6 dhcp interface
VLAN 100 is in client mode
  Configuration:
    Statefull Service is enabled (rapid-commit)
    Auto-Configuration is enabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is enabled
    Statefull Service is available
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  IPv6 Address Information:
    IA NA: IA ID 0x00040001, T1 120, T2 192
    IPv6 Address: 30e0::12:45:11
      preferred lifetime: 300, valid lifetime: 54333
      expires at Nov 08 2002 09:11 (54331 seconds)
      renew for address will be sent in 54301 seconds
    IPv6 Address: 3012::13:af:25
      preferred lifetime: 280, valid lifetime: 51111
      expires at Nov 08 2002 08:17 (51109 seconds)
```

```
      renew for address will be sent in 5101 seconds
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 105 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is disabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is enabled
    Statefull Service is not available (IPv6 routing is enabled)
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 107 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is enabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is enabled
    Statefull Service is not available (IPv6 routing is enabled)
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 110 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is disabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
```

```
    DHCP Operational mode is disabled (IPv6 is not enabled)
VLAN 1000 is in client mode
 Configuration:
    Statefull Service is enabled
    Auto-Configuration is enabled
    Information Refresh Time: 86400 seconds
    Information Refresh Minimum Time: 600 seconds
  State:
    DHCP Operational mode is disabled (Interface status is DOWN)
  DHCP server:
    Address: FE80::204:FCFF:FEA1:7439
    DUID: 000300010002FCA17400
    Preference: 20
  Stateless Information:
    Information Refresh Time:  86400 seconds
    expires at Nov 08 2002 08:17 (51109 seconds)
    DNS Servers: 1001::1, 2001::10
    DNS Domain Search List: company.com beta.org
    SNTP Servers: 2004::1
    POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
    Configuration Server: config.company.com
    Configuration Path Name: qqq/config/aaa_config.dat
    Indirect Image Path Name: qqq/config/aaa_image_name.txt
VLAN 1010 is in relay mode
  DHCP Operational mode is enabled
  Relay source interface: VLAN 101
  Relay destinations:
    2001:001:250:A2FF:FEBF:A056
    FE80::250:A2FF:FEBF:A056 via FastEthernet 1/0/10
```



CHAPTER 17

DNS Client Commands

This chapter contains the following sections:

- clear host, on page 305
- ip domain lookup, on page 306
- ip domain name, on page 306
- ip domain polling-interval, on page 307
- ip domain retry, on page 308
- ip domain timeout, on page 309
- ip host, on page 309
- ip name-server, on page 310
- show hosts, on page 311

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, on page 309 command.

To delete a static hostname-to-address mappings in the DNS hostname cache, use the **no** ip host, on page 309 command.

Example

The following example deletes all dynamic entries from the DNS client name-to-address cache.

```
switchxxxxxx# clear host *
```

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

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
```

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
```

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:

```
switchxxxxxx(config)# ip domain polling-interval 100
```

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 1.

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:

```
switchxxxxxx(config)# ip domain retry 10
```

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 2 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:

```
switchxxxxxx(config)# ip domain timeout 50
```

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 *hostname* [*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.

```
switchxxxxxx(config)# ip host accounting.website.com 176.10.23.1
```

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:

```
switchxxxxxx(config)# ip name-server 172.16.1.111 172.16.1.2 2001:0DB8::3
```

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 mode

Default Configuration

Default is **all**.

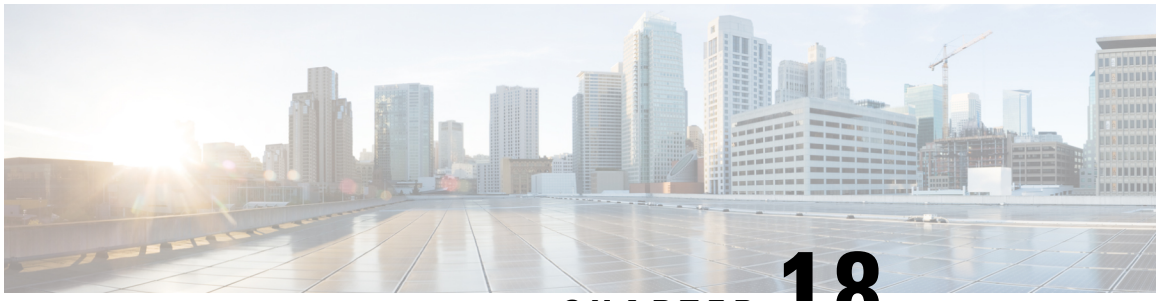
User Guidelines

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:

```
switchxxxxxx# 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
```



CHAPTER 18

DoS Commands

This chapter contains the following sections:

- security-suite deny fragmented, on page 313
- security-suite deny icmp, on page 314
- security-suite deny martian-addresses, on page 315
- security-suite deny syn, on page 317
- security-suite deny syn-fin, on page 318
- security-suite dos protect, on page 318
- security-suite dos syn-attack, on page 319
- security-suite enable, on page 320
- security-suite syn protection mode, on page 321
- security-suite syn protection recovery, on page 322
- security-suite syn protection threshold, on page 323
- show security-suite configuration, on page 323
- show security-suite syn protection, on page 324

security-suite deny fragmented

To discard IP fragmented packets from a specific interface, use the **security-suite deny fragmented** Interface (Ethernet, Port Channel) Configuration mode command.

To permit IP fragmented packets, use the **no** form of this command.

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

- **add** *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 (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 323 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 gi1/0/1
switchxxxxxx(config-if)# security-suite deny fragmented add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny icmp

To discard ICMP echo requests from a specific interface (to prevent attackers from knowing that the device is on the network), use the **security-suite deny icmp** Interface (Ethernet, Port Channel) Configuration mode command.

To permit echo requests, use the **no** form of this command.

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 (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 323 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 gi1/0/1
switchxxxxxx(config-if)# security-suite deny icmp add any /32
To perform this command, DoS Prevention must be enabled in the per-interface mode.
```

security-suite deny martian-addresses

To deny packets containing system-reserved IP addresses or user-defined IP addresses, use the **security-suite deny martian-addresses** Global Configuration mode command.

To restore the default, use the **no** form of this command.

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, show security-suite configuration, on page 323 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 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
```

security-suite deny syn

To block the creation of TCP connections from a specific interface, use the **security-suite deny syn** Interface (Ethernet, Port Channel) Configuration mode command. This a complete block of these connections.

To permit creation of TCP connections, use the **no** form of this command.

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**, 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 (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 323 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 gi1/0/1
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.
```

security-suite deny syn-fin

To drop all ingressing TCP packets in which both SYN and FIN are set, use the **security-suite deny syn-fin** Global Configuration mode command.

To permit TCP packets in which both SYN and FIN are set, use the **no** form of this command.

Syntax

security-suite deny syn-fin

no security-suite deny syn-fin

Parameters

This command has no arguments or keywords.

Default Configuration

The feature is enabled 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 syn-fin
```

security-suite dos protect

To protect the system from specific well-known Denial of Service (DoS) attacks, use the **security-suite dos protect** Global Configuration mode command. There are three types of attacks against which protection can be supplied (see parameters below).

To disable DoS protection, use the **no** form of this command.

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, show security-suite configuration, on page 323 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
```

security-suite dos syn-attack

To rate limit Denial of Service (DoS) SYN attacks, use the **security-suite dos syn-attack** Interface Configuration mode command. This provides partial blocking of SNY packets (up to the rate that the user specifies).

To disable rate limiting, use the **no** form of this command.

Syntax

security-suite dos syn-attack *syn-rate* {***any*** **|** *ip-address*} {*mask* | *prefix-length*}

no security-suite dos syn-attack {***any*** **|** *ip-address*} {*mask* | *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 (Ethernet, Port Channel) Configuration mode

User Guidelines

For this command to work, show security-suite configuration, on page 323 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 gi1/0/1
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.
```

security-suite enable

To enable the security suite feature and setting, use the **security-suite enable** Global Configuration mode command. The security suite feature supports protection against various types of attacks. To restore the default configuration, use the **no** form of this command.

Syntax

security-suite enable [**global-rules-only | interface-rules-only**]

no security-suite enable

Parameters

- **global-rules-only**—(Optional) Specifies that device will support only global level (and not interface level) security suite commands). 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.
- **interface-rules-only**—(Optional) Specifies that device will support only interface level security suite command (See details in user guidelines below). This mode cannot be enabled if an ACL is applied to any interface on device.
- **(none)** - If no keyword is used, security-suite commands can be used both globally and per-interface.This mode cannot be enabled if an ACL is applied to any interface on device.

Default Configuration

The security suite feature is disabled.

If neither **global-rules-only** or **interface-rules-only** are specified, the default is to enable security-suite globally and per interfaces.

Command Mode

Global Configuration mode

User Guidelines

Use this command to enable the ability to define security suite settings, and to determine the type of settings that can be enabled (only global level rules, only interface level rules or both types). When security-suite is enabled, the following commands can be used, depending on the mode set by user:

When this command is used, hardware resources are reserved. The number of resources reserved depends on the mode specified in command (**global-rules-only**, **interface-rules-only** or no mode (meaning both types)). Resources are released when the **no security-suite enable** command is entered.

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.

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 gi1/0/1
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 gi1/0/1
switchxxxxxx(config-if)# security-suite dos syn-attack 199 any /10
switchxxxxxx(config-if)#
```

security-suite syn protection mode

To set the TCP SYN protection mode, use the **security-suite syn protection mode** Global Configuration mode command.

To set the TCP SYN protection mode to default, use the **no** form of this command.

Syntax

security-suite syn protection mode {disabled | report | block}

no security-suite syn protection mode

Parameters

- **disabled**—Feature is disabled
- **report**—Feature reports about TCP SYN traffic per port (including rate-limited SYSLOG message when an attack is identified)

- **block**—TCP SYN traffic from attacking ports destined to the local system is blocked, and a rate-limited SYSLOG message (one per minute) is generated

Default Configuration

The default mode is block.

Command Mode

Global Configuration mode

User Guidelines

On ports in which an ACL is defined (user-defined ACL etc.), this feature cannot block TCP SYN packets. In case the protection mode is block but SYN Traffic cannot be blocked, a relevant SYSLOG message will be created, e.g.: “port gi1/0/1 is under TCP SYN attack. TCP SYN traffic cannot be blocked on this port since the port is bound to an ACL.”

Example 1: The following example sets the TCP SYN protection feature to report TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode report
```

Example 2: The following example sets the TCP SYN protection feature to block TCP SYN attack on ports in case an attack is identified from these ports.

```
switchxxxxxx(config)# security-suite syn protection mode block
```

security-suite syn protection recovery

To set the time period for the SYN Protection feature to block an attacked interface, use the **security-suite syn protection period** Global Configuration mode command.

To set the time period to its default value, use the **no** form of this command.

Syntax

security-suite syn protection recovery timeout

no security-suite syn protection recovery

Parameters

timeout—Defines the timeout (in seconds) by which an interface from which SYN packets are blocked gets unblocked. Note that if a SYN attack is still active on this interface it might become blocked again. (Range: 10-600)

Default Configuration

The default timeout is 60 seconds.

Command Mode

Global Configuration mode

User Guidelines

If the timeout is modified, the new value will be used only on interfaces which are not currently under attack.

Example

The following example sets the TCP SYN period to 100 seconds.

```
switchxxxxxx(config)# security-suite syn protection recovery 100
```

security-suite syn protection threshold

To set the threshold for the SYN protection feature, use the **security-suite syn protection threshold** Global Configuration mode command.

To set the threshold to its default value, use the **no** form of this command.

Syntax

security-suite syn protection threshold syn-packet-rate

no security-suite syn protection threshold

Parameters

syn-packet-rate—defines the rate (number of packets per second) from each specific port that triggers identification of TCP SYN attack. (Range: 20-200)

Default Configuration

The default threshold is 80pps (packets per second).

Command Mode

Global Configuration mode

Example

The following example sets the TCP SYN protection threshold to 40 pps.

```
switchxxxxxx(config)# security-suite syn protection threshold 40
```

show security-suite configuration

To display the security-suite configuration, use the **show security-suite configuration** switchxxxxxx> command.

Syntax

show security-suite configuration

Command Mode

User 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)
-----------------        --------------           --------------
gi1/0/1                  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
----------------         --------------           --------------
gi1/0/2                  176.16.23.0\24           FTP

ICMP filtering

Interface                IP Address
---------------          --------------
gi1/0/2                  176.16.23.0\24

Fragmented packets filtering

Interface                IP Address
--------------           --------------
gi1/0/2                  176.16.23.0\24
```

show security-suite syn protection

To display the SYN Protection feature configuration and the operational status per interface-id, including the time of the last attack per interface, use the **show security-suite syn protection** switchxxxxxx> command.

Syntax

show security-suite syn protection [interface-id]

Parameters

interface-id—(Optional) Specifies an interface-ID. The interface-ID can be one of the following types: Ethernet port of Port-Channel.

Command Mode

User EXEC mode

User Guidelines

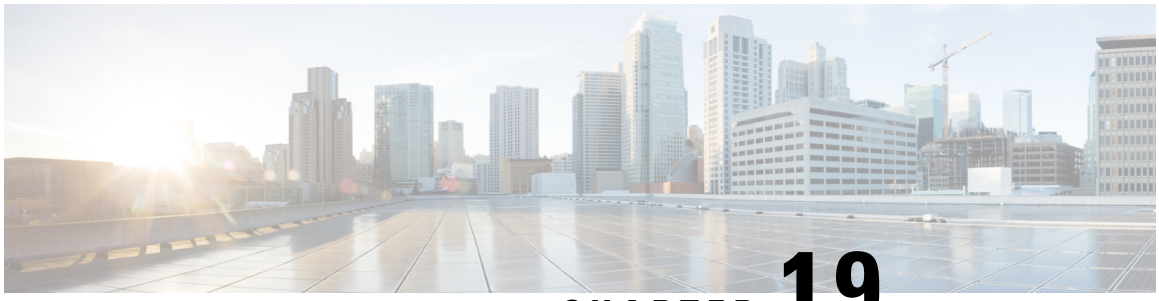
Use the Interface-ID to display information on a specific interface.

Example

The following example displays the TCP SYN protection feature configuration and current status on all interfaces. In this example, port gi1/0/2 is attacked but since there is a user-ACL on this port, it cannot become blocked so its status is Reported and not Blocked and Reported.

```
switchxxxxxx# show security-suite syn protection
Protection Mode: Block
Threshold: 40 Packets Per Second
Period: 100 Seconds
```

Interface Name	Current Status	Last Attack
gi1/0/1	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported
gi1/0/2	Attacked	19:58:22.289 PDT Feb 19 2012 Reported
gi1/0/3	Attacked	19:58:22.289 PDT Feb 19 2012 Blocked and Reported



CHAPTER 19

EEE Commands

This chapter contains the following sections:

- eee enable (global), on page 327
- eee enable (interface), on page 328
- eee lldp enable, on page 328
- show eee, on page 329

eee enable (global)

To enable the EEE mode globally, use the **eee enable** Global Configuration command. To disable the mode, use the **no** format of the command.

Syntax

eee enable

no eee enable

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

In order for EEE to work, the device at the other end of the link must also support EEE and have it enabled. In addition, for EEE to work properly, auto-negotaition must be enabled; however, if the port speed is negotiated as 1Giga, EEE always works regardless of whether the auto-negotiation status is enabled or disabled.

If auto-negotiation is not enabled on the port and its speed is less than 1 Giga, the EEE operational status is disabled.

Example

```
switchxxxxxx(config)# eee enable
```

eee enable (interface)

To enable the EEE mode on an Ethernet port, use the **eee enable** Interface Configuration command. To disable the mode, use the **no** format of the command.

Syntax

eee enable

no eee enable

Parameters

This command has no arguments or keywords.

Default Configuration

EEE is enabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

If auto-negotiation is not enabled on the port and its speed is 1 Giga, the EEE operational status is disabled.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# eee enable
```

eee lldp enable

To enable EEE support by LLDP on an Ethernet port, use the **eee lldp enable** Interface Configuration command. To disable the support, use the **no** format of the command.

Syntax

eee lldp enable

no eee lldp enable

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Enabling EEE LLDP advertisement enables devices to choose and change system wake-up times in order to get the optimal energy saving mode.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# eee lldp enable
```

show eee

Use the **show eee** EXEC command to display EEE information.

Syntax

show eee *[interface-id]*

Parameters

interface-id—(Optional) Specify an Ethernet port.

Defaults

None

Command Mode

Privileged EXEC mode

User Guidelines

If the port is a 10G port, but the link speed is 1G, the EEE Remote status cannot be resolved (and displayed).

Example 1 - The following displays brief Information about all ports.

```
switchxxxxxx# show eee
EEE globally enabled
EEE Administrate status is enabled on ports: gi1/0/1-2, gi1/0/4
EEE Operational status is enabled on ports: gi1/0/1-2, gi1/0/4
EEE LLDP Administrate status is enabled on ports: gi1/0/1-3
EEE LLDP Operational status is enabled on ports: gi1/0/1-2
```

Example 2 - The following is the information displayed when a port is in the Not Present state; no information is displayed if the port supports EEE.

```
switchxxxxxx# show eee gi1/0/1
Port Status: notPresent
```

```
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 3 - The following is the information displayed when the port is in status DOWN.

```
switchxxxxxx# show eee gi1/0/1
Port Status: DOWN
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 4 - The following is the information displayed when the port is in status UP and does not support EEE.

```
switchxxxxxx# show eee gi1/0/2
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Administrate status: enabled
EEE LLDP Administrate status: enabled
```

Example 5 - The following is the information displayed when the neighbor does not support EEE.

```
switchxxxxxx# show eee gi1/0/4
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: disabled
EEE Administrate status: enabled
EEE Operational status: disabled (neighbor does not support)
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

Example 6 - The following is the information displayed when EEE is disabled on the port.

```
switchxxxxxx# show eee gi1/0/1
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Administrate status: disabled
EEE Operational status: disabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: disabled
```

Example 7 - The following is the information displayed when EEE is running on the port, and EEE LLDP is disabled.

```
switchxxxxxx# show eee gi1/0/2
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: disabled
EEE LLDP Operational status: disabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
```

Example 8 - The following is the information displayed when EEE and EEE LLDP are running on the port.

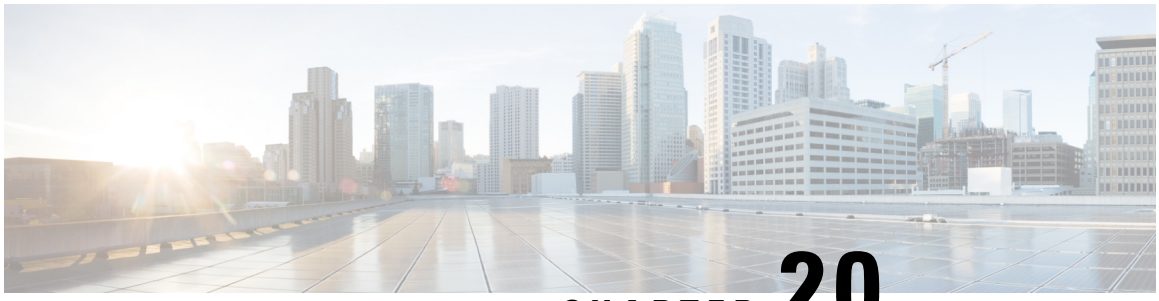
```
switchxxxxxx# show eee gi1/0/3
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```

Example 9 - The following is the information displayed when EEE is running on the port, EEE LLDP is enabled but not synchronized with the remote link partner.

```
switchxxxxxx# show eee gi1/0/4
Port Status: up
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status:  disabled
Resolved Tx Timer: 64
Local Tx Timer: 64
Resolved Rx Timer: 16
Local Rx Timer: 16
```

Example 10 - The following is the information displayed when EEE and EEE LLDP are running on the port.

```
switchxxxxxx# show eee gi1/0/3
Port Status: UP
EEE capabilities:
Speed 10M: EEE not supported
Speed 100M: EEE supported
Speed 1G: EEE supported
Speed 10G: EEE not supported

Current port speed: 1000Mbps
EEE Remote status: enabled
EEE Administrate status: enabled
EEE Operational status: enabled
EEE LLDP Administrate status: enabled
EEE LLDP Operational status: enabled
Resolved Tx Timer: 10usec
Local Tx Timer: 10 usec
Remote Rx Timer: 5 usec
Resolved Timer: 25 usec
Local Rx Timer: 20 usec
Remote Tx Timer: 25 usec
```



CHAPTER 20

Ethernet Configuration Commands

This chapter contains the following sections:

- interface, on page 334
- interface range, on page 334
- shutdown, on page 335
- operation time, on page 336
- description, on page 337
- speed, on page 337
- duplex, on page 338
- negotiation, on page 339
- flowcontrol , on page 340
- mdix, on page 340
- back-pressure, on page 341
- port jumbo-frame, on page 341
- link-flap prevention, on page 342
- clear counters, on page 343
- set interface active, on page 343
- errdisable recovery cause, on page 344
- errdisable recovery interval, on page 345
- errdisable recovery reset, on page 345
- show interfaces configuration, on page 346
- show interfaces status, on page 347
- show interfaces advertise, on page 348
- show interfaces description, on page 349
- show interfaces counters, on page 350
- show ports jumbo-frame, on page 352
- show link-flap prevention, on page 352
- show errdisable recovery, on page 353
- show errdisable interfaces, on page 353
- clear switchport monitor, on page 354
- show switchport monitor, on page 354

interface

To enter Interface configuration mode in order to configure an interface, use the **interface** Global Configuration mode command.

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, Bluetooth, IP interface or tunnel.

Command Mode

Global Configuration mode

Example 1—For Ethernet ports:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#
```

Example 2—For port channels (LAGs):

```
switchxxxxxx(config)# interface po1
switchxxxxxx(config-if)#
```

interface range

To execute a command on multiple ports at the same time, use the **interface range** command.

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

Command Mode

Interface (Ethernet, Port Channel, VLAN) Configuration 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 gi1/0/1-4
switchxxxxxx(config-if-range)#
```

shutdown

To disable an interface, use the **shutdown** Interface Configuration mode command. To restart a disabled interface, use the **no** form of this command.

Syntax

shutdown

no shutdown

Parameters

This command has no arguments or keywords.

Default Configuration

The interface is enabled.

Command Mode

Interface Configuration mode

User Guidelines

The shutdown command set a value of ifAdminStatus (see RFC 2863) to DOWN. When ifAdminStatus is changed to DOWN, ifOperStatus will be also changed to DOWN.

The DOWN state of ifOperStatus means that the interface does not transmit/receive messages from/to higher levels. For example, if you shut down a VLAN, on which an IP interface is configured, bridging into the VLAN continues, but the switch cannot transmit and receive IP traffic on the VLAN.

Notes:

- If the switch shuts down an Ethernet port it additionally shuts down the port MAC sublayer too.
- If the switch shuts down a port channel it additionally shuts down all ports of the port channel too.

Example 1—The following example disables gi1/0/4 operations.

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

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

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  no shutdown
switchxxxxxx(config-if)#
```

Example 3—The following example shuts down vlan 100.

```
switchxxxxxx(config)#  interface vlan 100
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

Example 4—The following example shuts down tunnel 1.

```
switchxxxxxx(config)#  interface tunnel 1
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

Example 5—The following example shuts down Port Channel 3.

```
switchxxxxxx(config)#  interface po3
switchxxxxxx(config-if)#  shutdown
switchxxxxxx(config-if)#
```

operation time

To control the time that the port is up, use the **operation time** Interface (Ethernet, Port Channel) Configuration mode command. To cancel the time range for the port operation time, use the **no** form of this command.

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 (Ethernet, Port Channel) Configuration 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 gi1/0/1.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  operation time morning
```

description

To add a description to an interface, use the **description** Interface Configuration mode command. To remove the description, use the **no** form of this command.

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 (Ethernet, Port Channel, Bluetooth) Configuration mode

Example

The following example adds the description 'SW#3' to gi1/0/4.

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  description SW#3
```

speed

To configure the speed of a given Ethernet interface when not using auto-negotiation, use the **speed** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

speed {**100** | **1000** | **2500** | **5000** | **10000**}

no speed

Parameters

- **100**—Forces 100 Mbps operation
- **1000**—Forces 1000 Mbps operation
- **2500**—Forces 2500 Mbps operation
- **5000**—Forces 5000 Mbps operation
- **10000**—Forces 10000 Mbps operation

Default Configuration

The port operates at its maximum speed capability.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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 gi1/0/4 to 100 Mbps operation.

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  speed 100
```

duplex

To configure the full/half duplex operation of a given Ethernet interface when not using auto-negotiation, use the **duplex** Interface (Ethernet, Port Channel) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet) Configuration mode

Example

The following example configures gi1/0/1 to operate in full duplex mode.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  duplex full
```

negotiation

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

Syntax

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

no negotiation

Parameters

- **Capability**—(Optional) Specifies the capabilities to advertise. (Possible values: 10h, 10f, 100h,100f, 1000f, 2500f, 5000f, 10000f).

  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

  2500f—Advertise 2500 full-duplex

  - **5000f**—Advertise 5000 full-duplex
  - **10000f**—Advertise 10000 full-duplex

- **Preferred**—(Optional) 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 slave mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables auto-negotiation on gi1/0/1.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  negotiation
```

flowcontrol

To configure the Flow Control on a given interface, use the **flowcontrol** Interface (Ethernet, Port Channel) Configuration mode command. To disable Flow Control, use the **no** form of this command.

Syntax

flowcontrol *{***on** | **off***}*

no flowcontrol

Parameters

- **on**—Enables Flow Control.
- **off**—Disables Flow Control.

Default Configuration

Flow control is set to Disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables Flow Control on port gi1/0/1

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  flowcontrol on
```

mdix

To enable cable crossover on a given interface, use the **mdix** Interface (Ethernet) Configuration mode command. To disable cable crossover, use the **no** form of this command.

Syntax

mdix *{***on** | **auto***}*

no mdix

Parameters

- **on**—Enables manual MDIX.
- **auto**—Enables automatic MDI/MDIX.

Default Configuration

The default setting is Auto.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example enables automatic crossover on port gi1/0/1.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  mdix auto
```

back-pressure

To enable back pressure on a specific interface, use the **back-pressure** Interface (Ethernet) Configuration mode command. To disable back pressure, use the **no** form of this command.

Syntax

back-pressure

no back-pressure

Parameters

This command has no arguments or keywords.

Default Configuration

Back pressure is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Back-pressure cannot be enabled when EEE is enabled.

Example

The following example enables back pressure on port gi1/0/1.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  back-pressure
```

port jumbo-frame

To enable jumbo frames on the device, use the **port jumbo-frame** Global Configuration mode command. To disable jumbo frames, use the **no** form of this command.

Syntax

port jumbo-frame

no port jumbo-frame

Parameters

This command has no arguments or keywords.

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
```

link-flap prevention

To enable setting a physical interface to err-disable state due to excessive link flapping, use the **link-flap prevention** Global Configuration mode command. Use the **no** form of this command to restore the default configuration.

Syntax

link-flap prevention {**enable** | **disable**}

no link-flap prevention

Parameters

enable—Enables Link-flap Prevention.

disable—Disables Link-flap Prevention.

Default Configuration

Link-flap prevention is enabled on the device.

Command Mode

Global Configuration mode

User Guidelines

This command will shutdown Ethernet (Physical) interfaces if the interface experienced, for a duration of 10 seconds, 3 link flaps (link status changes) within each second.

Example

The following example enables link-flap prevention on the device.

```
switchxxxxxx(config)#  link-flap prevention
```

clear counters

To clear counters on all or on a specific interface, use the **clear counters** Privileged EXEC mode command.

Syntax

clear counters *[interface-id]*

Parameters

interface-id—(Optional) 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

Privileged EXEC mode

Example

The following example clears the statistics counters for gi1/0/1.

```
switchxxxxxx#  clear counters gi1/0/1
```

set interface active

To reactivate an interface that was shut down, use the **set interface active** Privileged EXEC mode command.

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

Privileged 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 gi1/0/1.

```
switchxxxxxx#  set interface active gi1/0/1
```

errdisable recovery cause

To enable automatic re-activation of an interface after an Err-Disable shutdown, use the **errdisable recovery cause** Global Configuration mode command. To disable automatic re-activation, use the **no** form of this command.

Syntax

errdisable recovery cause {**all** | **port-security** | **dot1x-src-address** | **acl-deny** | **stp-bpdu-guard** | **stp-loopback-guard** | l**oopback-detection | udld | storm-control | link-flap** }

no errdisable recovery cause {**all** | **port-security** | **dot1x-src-address** | **acl-deny** | **stp-bpdu-guard** | **stp-loopback-guard** | l**oopback-detection** | **udld | storm-control | link-flap** }

Parameters

- **all**—Enables the error recovery mechanism for all reasons described below.
- **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 the STP BPDU Guard Err-Disable state.
- **stp-loopback-guard**—Enables the error recovery mechanism for the STP Loopback Guard Err-Disable state.
- **loopback-detection**—Enables the error recovery mechanism for the Loopback Detection Err-Disable state.
- **udld**—Enables the error recovery mechanism for the UDLD Shutdown state.
- **storm-control**—Enables the error recovery mechanism for the Storm Control Shutdown state.
- **link-flap**—Enables the error recovery mechanism for the link-flap prevention Err-Disable state.

Default Configuration

Automatic re-activation is disabled, except for link-flap reason where automatic re-creation is enabled by default.

Command Mode

Global Configuration mode

Example

The following example enables automatic re-activation of an interface after all states.

```
switchxxxxxx(config)#  errdisable recovery cause all
```

errdisable recovery interval

To set the error recovery timeout intervalse the **errdisable recovery interval** Global Configuration mode command. To return to the default configuration, use the **no** form of this command.

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
```

errdisable recovery reset

To reactivate one or more interfaces that were shut down by a given application, use the **errdisable recovery reset** Privileged EXEC mode command. A single interface, multiple interfaces or all interfaces can be specified.

Syntax

errdisable recovery reset {**all** | **port-security** | **dot1x-src-address** | **acl-deny** |**stp-bpdu-guard** | **stp-loopback-guard** | l**oopback-detection | udld | storm-control | link-flap | interface** *interface-id*}

Parameters

- **all**—Reactivate all interfaces regardless of their state.

- **port-security**—Reactivate all interfaces in the Port Security Err-Disable state.
- **dot1x-src-address—**Reactivate all interfaces in the 802.1x Err-Disable state.
- **acl-deny**—Reactivate all interfaces in the ACL Deny Err-Disable state.
- **stp-bpdu-guard**—Reactivate all interfaces in the STP BPDU Guard Err-Disable state.
- **stp-loopback-guard**—Reactivate all interfaces in the STP Loopback Guard Err-Disable state.
- **loopback-detection**—Reactivate all interfaces in the Loopback Detection Err-Disable state.
- **udld**—Reactivate all interfaces in the UDLD Shutdown state.
- **storm-control**—Reactivate all interfaces in the Storm Control Shutdown state.
- **link-flap**—Reactivate all interfaces in the link-flap prevention Err-Disable state.
- **interface** *interface-id*—Reactivate interfaces that were configured to be active, but were shut down by the system.

Command Mode

Privileged EXEC mode

Example 1—The following example reactivates interface gi1/0/1:

```
switchxxxxxx# errdisable recovery reset interface gi1/0/1
```

Example 2—The following example reactivates all interfaces regardless their state:

```
switchxxxxxx# errdisable recovery reset all
```

Example 3—The following example enables all interfaces in the port security Err-Disable state

```
switchxxxxxx# errdisable recovery reset port-security
```

show interfaces configuration

To display the configuration for all configured interfaces or for a specific interface, use the **show interfaces configuration** Privileged EXEC mode command.

Syntax

show interfaces configuration *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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

Privileged 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
------ -------- ------  -----  -------- -------  -----  --------  ----
gi1/0/1 1G-Copper   Full    1000   Enabled  Off      Up     Disabled  Off
gi1/0/2 1G-Copper   Full    1000   Disabled Off      Up     Disabled  Off
gi1/0/2 10G-Copper  Full    10000  Disabled Off      Up     Disabled  Off
gi1/0/3 10G-Copper  Full    2500   Disabled Off      Up     Disabled  Off
gi1/0/4 10G-Copper  Full    5000   Disabled Off      Up     Disabled  Off
                                  Flow      Admin
PO      Type   Speed  Neg        Control   State
------  ------ -----  --------   -------   -----
Po1                   Disabled   Off       Up
```

show interfaces status

To display the status of all interfaces or of a specific interface, use the **show interfaces status** Privileged EXEC mode command.

Syntax

show interfaces status *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) Displays information for non-present ports in addition to present ports.

Command Mode

Privileged 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
------ ---------- ------  ----- -------- ----  ------ -------- --
gi1/0/1  1G-Copper  Full   1000  Disabled Off   Up     Disabled Off
gi1/0/2  1G-Copper  --     --     --      --    Down   --       --
te1/0/1  10G-Copper --     2500   --      --    Down   --       --
```

```
                                        Flow     Link
PO     Type      Duplex Speed  Neg      control  State
-----  --------  ------ -----  -------- -------  ------
Po1    1G        Full   10000  Disabled Off      Up
*: The interface was suspended by the system.
```

show interfaces advertise

To display auto-negotiation advertisement information for all configured interfaces or for a specific interface, use the **show interfaces advertise** Privileged EXEC mode command.

Syntax

show interfaces advertise *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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

Examples

The following examples display auto-negotiation information.

```
switchxxxxxx#  show interfaces advertise

Port    Type        Neg     Prefered Operational Link Advertisement
----    ----------- ------  -------  ----------------------------
gi1/0/1 1G-Copper   Enable  Master   1000f, 100f, 10f, 10h
gi1/0/2 1G-Copper   Enable  Slave    1000f
tw1/03  2.5G-Copper Enable           2500f, 1000f, 100f, 100h
                            Slave
te1/0/1 10G-Copper  Enable  Slave    10000f, 5000f, 2500f,1000f
```

```
switchxxxxxx#  show interfaces advertise gi1/0/1
Port:gi1/0/1
Type: 1G-Copper
Link state: Up
Auto Negotiation: enabled
Preference: Master
```

Admin Local link Advertisement		10h	10f	100h	100f	1G	2.5G
Oper Local link Advertisement		---	---	----	----	-----	-----
Remote Local link Advertisement		yes	yes	yes	yes	yes	no
Priority Resolution		yes	yes	yes	yes	yes	no
		no	no	yes	yes	yes	no
		-	-	-	-	yes	-

```
switchxxxxxx#  show interfaces advertise gi1/0/1
Port: gi1/0/1
Type: 1G-Copper
Link state: Up
Auto negotiation: disabled.
```

show interfaces description

To display the description for all configured interfaces or for a specific interface, use the **show interfaces description** Privileged EXEC mode command.

Syntax

show interfaces description *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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

Privileged EXEC mode

Example

The following example displays the description of all configured interfaces.

```
switchxxxxxx#  show interfaces description
```

Port ------ gi1/0/1 gi1/0/2 gi1/0/3 gi1/0/4	Descriptions ---------- Port that should be used for management only
PO ---- Po1	Description ----------- Output

show interfaces counters

To display traffic seen by all the physical interfaces or by a specific interface, use the **show interfaces counters** Privileged EXEC mode command.

Syntax

show interfaces counters *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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

Privileged EXEC mode

Example

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

```
switchxxxxxx#  show interfaces counters gi1/0/1
Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------- ------------ ------------ ------------ ------------
gi1/0/1           0            0            0            0
Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------- ------------ ------------ ------------ ------------
gi1/0/1           0            1            35          7051
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.

Field	Description
InMcastPkts	Number of received Unicast packets.
InBcastPkts	Number of received broadcast packets.
OutOctets	Number of transmitted octets.
OutUcastPkts	Number of transmitted Unicast packets.
OutMcastPkts	Nmber of transmitted Unicast 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.

show ports jumbo-frame

To display whether jumbo frames are enabled on the device, use the **show ports jumbo-frame** Privileged EXEC mode command.

Syntax

show ports jumbo-frame

Parameters

This command has no arguments or keywords.

Command Mode

Privileged 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
```

show link-flap prevention

To display whether link-flap prevention is enabled on the device, use the **show link-flap prevention** Privileged EXEC mode command.

Syntax

show link-flap prevention

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays whether link-flap prevention is enabled on the device.

```
switchxxxxxx#  show link-flap prevention
link-flap prevention is currently enabled on device
```

show errdisable recovery

To display the Err-Disable configuration of the device, use the **show errdisable recovery** Privileged EXEC mode command.

Syntax

show errdisable recovery

Parameters

This command has no arguments or keywords.

Command Mode

Privileged 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
loop-detection          Disable
udld                    Disable
storm control           Disable
link-flap              Disable
```

show errdisable interfaces

To display the Err-Disable state of all interfaces or of a specific interface, use the **show errdisable interfaces** Privileged EXEC mode command.

Syntax

show errdisable interfaces [*interface-id*]

Parameters

- **interface**—(Optional) Port or port-channel number.

Default Configuration

Display for all interfaces.

Command Mode

Privileged EXEC mode

Example

The following example displays the Err-Disable state of gi1/0/1.

```
switchxxxxxx#  show errdisable interfaces
Interface                Reason                       Time to recovery
(sec)
------------          ------------------              -------------
gi1/0/1                  port-security                       250
gi1/0/5                  acl-deny                            NA
```

clear switchport monitor

To clear monitored statistics on all or on a specific interface or interface list, use the **clear switchport monitor** Privileged EXEC mode command.

Syntax

clear switchport monitor *[interface-id-list]*

Parameters

interface-id-list—(Optional) Specifies a list of interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.

Default Configuration

All monitored statistics are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears the monitored statistics for gi1/0/1.

```
switchxxxxxx#  clear switchport monitor gi1/0/1
```

show switchport monitor

To display the monitored statistics gathered by a specific interface, use the **show switchport monitor** Privileged EXEC mode command.

Syntax

show switchport monitor *interface-id* {**seconds** | **minutes** | **hours** | **days** |**weeks**} *[***utilization** | **tx** | **rx** | **frames]**

show switchport monitor *interface-id* {***days*** |**weeks**}

show switchport monitor utilization *[interface-id]*

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **seconds**— last 20 samples, sampled every 15 seconds.
- **minutes** —last 60 samples, sampled every 60 seconds (every round minute according to system time).
- **hours** —last 24 samples, sampled every 60 minutes (every round hour according to system time).
- **days** —last 7 samples, sampled every 24 hours (midnight to midnight according to system time).
- **weeks** —last 12 samples, sampled every 7 days (midnight saturday to midnight saturday according to system time).
- **utilization** —shows per time frame the utilization calculated.
- **rx** —shows received counters statistics.
- **tx** —shows sent counters statistics.
- **frames** —show received counters statistics collected per packet size**.**

Default Configuration

Display monitored statistics for an interface or all interface in case of s**show switchport monitor *utilization*** command.

Command Mode

Privileged EXEC mode

User Guidelines

The **show switchport monitor *utilization*** is used to show a utilization summary per interface of the last time frame in each time frame(i.e. last minute, last hour, last day and last week).

The **show switchport monitor** *interface-id* is used to show monitored statistics samples collected per time frame and per counter types.

Example 1—The following example displays monitored statistics utilization seen by interface gi1/0/1.

```
switchxxxxxx#  show switchport monitor utilization gi1/0/1
```

Interface --------- gi1/0/1	Minutes Rx/TX utilization ------------ 95%	Hours Rx/TX utilization ----------- 80%	Days Rx/TX utilization ----------- 60%	Weeks Rx/TX utilization ----------- 20%

Example 2—The following example displays monitored Tx statistics gathered in minutes time frame seen by interface gi1/0/1.

```
switchxxxxxx#  show switchport monitor gi1/0/1 minutes tx
```

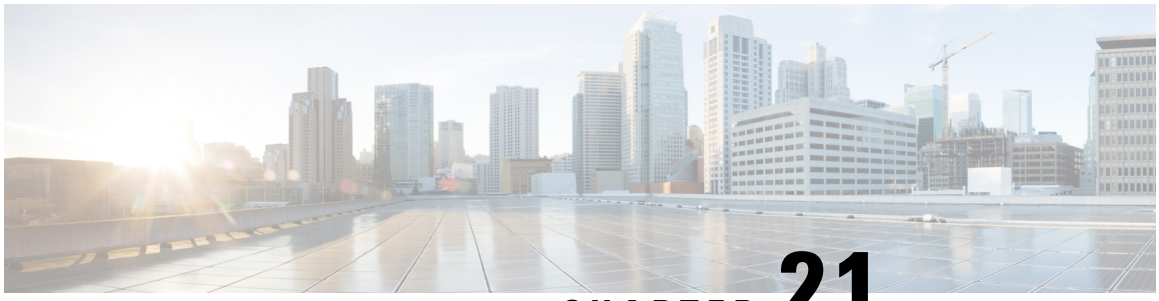
Time	Unicast frames Sent	Broadcast frames Sent	Multicast frames Sent	Good Octet Sent
----------	--------------	-----------	-----------	-------
04:22:00(~)	95%	80%	60%	20%
04:23:00	80%	70%	60%	50%

(~) Not all samples are available.

The following table describes the fields shown in the display.

Field	Description
Time	Time stamp of the current sample in system real time clock. For seconds, minutes and hours format is: hh:mm:ss. For days and weeks format is: <day of week> dd/mm/yy.
Good Octets Received	Number of received octets.
Good Unicast frames Received	Number of received Unicast packets.
Good Multicast frames Received	Number of received Unicast packets.
Good Broadcast frames Received	Number of received broadcast packets.
Good Octets Sent	Number of transmitted octets.
Good Unicast frames Sent	Number of transmitted Unicast packets.
Good Multicast frames Sent	Nmber of transmitted Unicast packets.
Good Broadcast frames Sent	Number of transmitted Broadcast packets.
Frames of 64 bytes	Number of received packets size of 64 bytes.
Frames of 65-127 bytes	Number of received packets size of 65-127 bytes.
Frames of 128-255 bytes	Number of received packets size of 128-255 bytes.
Frames of 256-511 bytes	Number of received packets size of 256-511 bytes.
Frames of 512-1023 bytes	Number of received packets size of 512-1023 bytes.
Frames of 1024-1518 bytes	Number of received packets size of 1024-1518 bytes.
Rx Error Frames Received	Number of frames received that are an integral number of octets in length but do not pass the FCS check.
Rx Utilization	Utilization in percentage for Received frames on the interface.
Tx Utilization	Utilization in percentage for Sent frames on the interface.

Field	Description
Rx/Tx Utilization	An average of the Rx Utilization and the Tx Utilization in percentage on the interface.



CHAPTER 21

File System Commands

This chapter contains the following sections:

- File Specification, on page 359
- System Flash Files, on page 362
- Flash File System on Stack, on page 363
- boot config, on page 363
- boot localization, on page 364
- boot system, on page 365
- cd, on page 366
- copy, on page 367
- delete, on page 368
- dir, on page 369
- mkdir, on page 370
- more, on page 371
- pwd, on page 371
- reload, on page 372
- rename, on page 373
- rmdir, on page 375
- service mirror-configuration, on page 375
- show bootvar / show version, on page 376
- show mirror-configuration service, on page 379
- show reload, on page 379
- show running-config, on page 380
- show startup-config, on page 381
- show diff-config, on page 382
- write, on page 382

File Specification

The files may be located on:

- Network: TFTP servers and/or SCP servers - Network files
- Active FLASH - Flash files

- mass-storage connected to a USB port of Active - USB files. Only one mass-storage is supported.

Note. Although inside the switch supports the File System on FLASH of all stack units the File System CLI commands allow access only to flash files on Active unit. Needed file synchronizations between Active unit and other units is performed by the switch automatically.

Uniform Resource Locators (URLs) are used to specify the location of a file or a directory. The URL has the following syntax:

<*url*> ::= **tftp://**<*location*>/<*file-path*> | **scp://**[<*username*>**:**<*password*>**@**]<*location*>/<*file-path*> | **usb://**<*file-path*> | **flash://**<*file-path*> | <*current-directory*>[/<*file-path*>] | <*higher-directory*>[/<*file-path*>] | <*file-path*>

<*username*> ::= string up to 70 characters

<*password*> :: = string up to 70 characters

<*location*> ::= <*ipv4-address*> | <*ipv6-address*> | <*dns-name*>

<*current-directory*> ::= [{**usb** | **flash**}**:**][**.**]

<*higher-directory*> ::= [{**usb** | **flash**}**:**]**..**

<*file-path*> ::= [<*directories-path*>/]<*filename*>

<*directories-path*> ::= <*directory-name*> | <*directories-path*>/<*directory-name*>

The maximum number of directories in <*directories-path*> is 16.

<*directory-name*> ::= string up to 63 characters

<*filename*> ::= string up to 63 characters

Filenames and directory names consist only of characters from the portable filename character set. The set includes the following characters:

- A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- a b c d e f g h i j k l m n o p q r s t u v w x y z
- <space>
- 0 1 2 3 4 5 6 7 8 9 . _ -

The last three characters are the <period>, <underscore>, and <hyphen> characters, respectively.

If an URL includes spaces it must be enclosed by the " characters.

For example:

"flash://aaa it/alpha/file 125"

The maximal length of URL is 160 characters

The following File systems are supported on USB:

- **FAT32**—Full support.
- **NTFS**—Partially support: read only.

The switch supports the following predefined URL aliases:

- **active-image**—The predefined URL alias specifies the Active Image file. This file has the following permissions:

  readable

  executable

- **inactive-image**—The predefined URL alias specifies the Inactive Image file. This file has the following permissions:

  readable

  executable

- **running-config**—The predefined URL alias specifies the Running Configuration File.
- **startup-config**—The predefined URL alias specifies the Startup Configuration File. This file has the following permissions:

  readable

- **localization**. The predefined URL alias specifies the Secondary Language Dictionary files. These files have the following permissions:

  readable

- **logging**. The predefined URL alias specifies the Syslog file. This file has the following permissions:

  readable

- **mirror-config**. The predefined URL alias specifies the Mirror Configuration file. This file has the following permissions:

  readable

Example 1. The following example specifies a file on TFTP server using an IPv4 address:

```
tftp://1.1.1.1/aaa/dat/file.txt
```

Example 2. The following example specifies a file on TFTP server using an IPv6 address:

```
tftp://3000:1:2::11/aaa/dat/file.txt
```

Example 3. The following example specifies a file on TFTP server using a DNS name:

```
tftp://files.export.com/aaa/dat/file.txt
```

Example 4. The following example specifies a file on FLASH:

```
flash://aaa/dat/file.txt
```

Example 5. The following example specifies files using the current directory:

```
./dat/file.txt
```

```
dat/file.txt
```

Example 6. The following example specifies a file using the higher directory:

```
../dat/file.txt
```

Example 7. The following example specifies a file on mass-storage device connected to the USB port:

```
usb://aaa/dat/file.txt
```

Example 8. The following example specifies files on mass-storage device connected to the USB port using the current directory:

```
usb:aaa/dat/file.txt
```

```
usb:./aaa/dat/file.txt
```

Example 9. The following example specifies a file on mass-storage device connected to the USB port using the higher directory:

```
usb:../aaa/dat/file.txt
```

System Flash Files

The system files used by the switch are in the **flash://system/** directory. A user cannot add, delete, and rename the system files and directories, a user cannot create new directories under the system directory.

The system files are divided to the following groups:

- Inner System files. The files are created by the switch itself. For example the Syslog file.
- Files installed/Uninstalled by user. This group includes the following files:

  Active and Inactive Images

  Startup Configuration

  Secondary Language Dictionary

Additionally, the following commands from previous versions can be used too:

Note. Reset to Factory Default removes all files from the FLASH except the following files:

- active-image
- inactive-image
- mirror-config
- localization

The **flash://system/** directory contains the following directories:

- **flash://system/images/**—The directory contains the Active and Inactive Image files.
- **flash://system/configuration/**—The directory contains the Startup and Mirror Configuration files.
- **flash://system/localization/**—The directory contains the Secondary Language Dictionary files.
- **flash://system/syslog/**—The directory contains the Syslog file.
- **flash://system/applications/**—The directory contains inner system files managed by the switch applications.

Flash File System on Stack

The CLI commands provide access only to files located on the Active unit FLASH. The switch performs automatically synchronization files between Active unit and Member units:

- The Standby unit's Flash File system is fully synchronized with the Active unit's Flash File System.
- For non-Standby Member units File system only the following files are synchronized:
  - Active Image file
  - Inactive Image file
  - Secondary Language Dictionary files
  - All other files and directories are deleted.

boot config

To install a file as Startup Configuration after reload, use the **boot config** command in Privileged EXEC mode. To uninstall the Startup configuration file, use the **no** form of this command.

Syntax

boot config *startup-config-url*

boot config running-config

boot config mirror-config

no boot config

Parameters

- ***startup-config-url*—**the url of a file. The predefined URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **boot config** *startup-config-url* command to install Startup Configuration from the *startup-config-url* file. The file must be a text file containing CLI commands. The command performs the following actions:

- Copies the file into the system directory **flash://system/configuration/**
- Converts the file format from the text format in the inner binary format.
- Installs the converted file as Startup Configuration. The previous Startup Configuration file is deleted.
- Installs Startup Configuration on Standby unit.

Use the **boot config running-config** command to install Startup Configuration from Running Configuration.

Use the **boot config mirror-config** command to install Startup Configuration from the Mirror Configuration file.

Use the **no boot config** command, to uninstall Startup Configuration. The uninstalled file is deleted.

Example 1. The following example installs Startup Configuration from a TFTP server:

```
switchxxxxxx#  boot config tftp://1.1.1./confiration-files/config-v1.9.dat
```

Example 2. The following example installs Startup Configuration from FLASH:

```
switchxxxxxx#  boot config flash://confiration-files/config-v1.9.dat
```

Example 3. The following example unsets the current Startup Configuration:

```
switchxxxxxx#  no boot config
```

Example 4. The following example installs Startup Configuration from the Running Configuration file:

```
switchxxxxxx#  boot config running-config
```

Example 5. The following example installs Startup Configuration from the Mirror Configuration file:

```
switchxxxxxx#  boot config mirror-config
```

boot localization

To install a file as the Secondary Language Dictionary file, use the **boot localization** command in Privileged EXEC mode. To remove all the installed language files, use the **no** form of this command.

Syntax

boot localization *dictionary-url*

no boot localization

Parameters

- ***dictionary***-url—the url of a file. The predefined URLs cannot be configured.

Default Configuration

Default language.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **boot localization** *dictionary-url* command to install aSecondary Language Dictionary from the *dictionary-url* file. The command performs the following actions:

- Copies the file into the system directory **flash://system/localization/**
- Validates installed file format and if the file language is supported by the device. If the file does not have the correct format, or if the file language is not supported by the device, the file is not copied and the command will finish with an error.
- Replaces the relevant language file on device with the installed file. Update of language file does not change the active secondary language used by web GUI user.
- Installs Secondary Language Dictionary relevant file on all the all other stack units.

Use the **no boot dictionary** command, to uninstall Secondary Language Dictionary. The uninstalled files are deleted.

Example 1. The following example installs the Secondary Language Dictionary file from a TFTP server:

```
switchxxxxxx#  boot localization tftp://196.1.1.1/web-dictionaries/germany-dictionary.lang
```

Example 2. The following example installs the Secondary Language Dictionary file from FLASH:

```
switchxxxxxx#  boot localization flash://web-dictionaries/germany-dictionary.lang
```

boot system

To install the system (active) image that the switch loads at startup, use the **boot system** command in Privileged EXEC mode.

Syntax

boot system *image-url*

boot system inactive-image

Parameters

- ***image-url***—The URL of a file. The predefined URLs cannot be configured.

Default Configuration

No default.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **boot system** *image-url* command to install a new active image from the *image-url* file. The command performs the following actions:

- Copies the file into the system directory **flash://system/image/**

- Validates its format. If the file does not have the correct image format the file is deleted and the command is finished with an error.
- Installs the copied file as the active image that will be used be loaded at startup. The previous active image file is save as inactive image. The previous inactive image is deleted.
- Installs the new active image in all stack units.

Use the **boot system inactive-image** command to set the inactive image as active one and the active image as inactive one.

The command installs the inactive image as active in all stack units.

Example 1. The following example sets a new active image from a TFTP server:

```
switchxxxxxx#  boot system tftp://145.21.2.3/image/image-v1-1.ros
```

Example 2. The following example sets a new active image from FLASH:

```
switchxxxxxx#  boot system flash://images/image-v1-1.ros
```

Example 3. The following example sets the inactive image:

```
switchxxxxxx#  boot system inactive-image
```

cd

To change the current directory or file system, use the **cd** command in User EXEC mode.

Syntax

cd *url*

Parameters

- ***url***—Specifies a directory on FLASH or on USB.

Default Configuration

The flash root directory (**flash://**)

Command Mode

User EXEC mode

User Guidelines

When a terminal session is started the current directory of the session is set to **flash://**. Use the **cd** command to change the current directory.

Example 1. The following example sets a new current directory on FLASH:

```
switchxxxxxx>  pwd
flash://
switchxxxxxx>  cd date/aaa
```

```
switchxxxxxx> pwd
flash://date/aaa
```

Example 2. The following example sets a new current directory on USB:

```
switchxxxxxx> pwd
flash://
switchxxxxxx> cd usb://
switchxxxxxx> pwd
usb://
```

copy

To copy any file from a source to a destination, use the **copy** command in Privileged EXEC mode.

Syntax

copy *src-url dst-url*

***copy** {**running-config** | **startup-config**} *dst-url*

copy {**running-config** | **startup-config**} *dst-url* [**exclude** | **include-encrypted** | **include-plaintext**]

copy *src-url* **running-config**

copy running-config startup-config

copy tech-support cbd usb://<*file-path*>

Parameters

- ***src-url***—The location URL of the source file to be copied. The predefined URL aliases can be configured.
- ***dst-url***—The URL of the destination file or the directory to be copied. The predefined URL aliases cannot be configured.
- **exclude**—The file does not include sensitive data in the file being copied.
- **include-encrypted**—The file includes sensitive data in its encrypted form. This secure option is applied by default, if no secure option is configured.
- **include-plaintext**—The file includes sensitive data in its plaintext form.
- **tech-support cbd** — Indicates that the source is the Cisco Business Dashboard (CBD) tech support information. If this source is selected, the destination can only be USB. If specified filename does not include the ".zip" suffix, this suffix will be added automatically to copied filename (full path length up to 160 characters).

Command Mode

Privileged EXEC mode

User Guidelines

The following guidelines are relevant:

- You cannot copy one network file to another network file.

- **Localization** is not supported as a predefined *src-url* or *dst-url*.
- Use the **copy** *src-url dst-url* command to copy any file. If the *dst-url* argument defines an existed flash file the command fails if this file does not have the writable permission. If the *dst-url* argument defines a directory file then the file is copied into the directory with the same name. No file format validation or conversion is performed. If the *src-url* argument and *dst-url* arguments define flash files the *dst-url* file will have the permissions of the *src-url* file. If the *src-url* argument defines a non-flash file and the *dst-url* argument defines a flash files the *dst-url* file will have the following permissions:
  - readable
  - writable
- Use the **copy** *src-url* **running-config** command to add a file to the Running Configuration file.

Example 1. The following example copies file file1 from the TFTP server 172.16.101.101 to the **flash://aaa/file1** file:

```
switchxxxxxx# copy tftp://172.16.101.101/file1 flash://aaa/file1
```

Example 2. The following example saves the Startup configuration file in the **tftp://172.16.101.101/config.txt** file:

```
*switchxxxxxx# copy startup-config tftp://172.16.101.101/config.txt or switchxxxxxx# copy
startup-config tftp://172.16.101.101/config.txt include-encrypted
```

Example 3. The following example copies the Running Configuration file to the Startup configuration:

```
switchxxxxxx# copy running-config startup-config
```

Note *

If ssd configuration in show running-config or startup-config reads “file SSD indicator **plaintext**”, the copied file will have sensitive information in **plaintext**.

If ssd configuration in show running-config or startup-config reads “file SSD indicator **encrypted** ”, the copied file will have sensitive information **encrypted**.

If ssd configuration in show running-config or startup-config reads “file SSD indicator **exclude** ”, the copied file will not include sensitive information will be **excluded.**

Example 4. The following example copies the Syslog file to a TFTP server:

```
switchxxxxxx# copy logging tftp://1.1.1.1/syslog.txt
```

Example 5. The following example copies a file from the mass-storage device connected to the USB port to Flash:

```
switchxxxxxx# copy usb://aaa/file1.txt flash://dir1/file2
```

delete

To delete a local file, use the **delete** command in Privileged EXEC mode.

Syntax

delete *url*

delete startup-config

Parameters

- ***url***—Specifies the local URL of the local file to be deleted. The predefined and network URLs cannot be configured.
- ***file-name***—Specifies the name of SNA user file to delete.

Command Mode

Privileged EXEC mode

User Guidelines

The **delete** *url* command cannot delete a network file.

Use the **delete startup-config** command to delete the Startup Configuration file.

Example 1. The following example deletes the file called ‘backup/config’ from FLASH:

```
switchxxxxxx# cd flash://backup/
switchxxxxxx# delete aaa.ttt
Delete flash://backup/aaa.ttt? [Y/N]Y
```

Example 2. The following example deletes the file called ‘aaa/config’ from the mass-storage device connected to the USB port:

```
switchxxxxxx# delete usb://aaa/config
Delete usb://aaa/config? [Y/N]Y
```

dir

To display a list of files on a file system, use the **dir** command in User EXEC mode.

Syntax

dir [*url*]

Parameters

- ***url***—Specifies the local URL of the directory to be displayed. The predefined and network URLs cannot be configured. If the argument is omitted the current directory is used.

Command Mode

User EXEC mode

User Guidelines

The command cannot be applied to a network directory.

Use the **dir** command without the argument to display the current directory.

Examples

The following example displays the **flash://mng/** directory:

```
switchxxxxxx> dir flash://mng/
Permissions
  d-directory
  r-readable
  w-writable
  x-executable
134560K of 520000K are free
Directory of flash://mng/
Permission  File Size     Last Modified      File Name
----------  ---------  --------------------  ------------------
 drw-         4720148  Dec 12 2010 17:49:36  bin
 -r--              60  Dec 12 2011 17:49:36  config-list
 -r--             160  Feb 12 2011 17:49:36  image-list
 -r-x         6520148  Nov 29 2010  7:12:30  image1
 -rw-            2014  Nov 20 2010  9:12:30  data
```

mkdir

To create a new directory, use the **mkdir** command in Privileged EXEC mode.

Syntax

mkdir *url*

Parameters

- *url*—Specifies the URL of the created directory. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The **mkdir** command cannot be applied to a network directory.

The **mkdir** command cannot create a directory into the **flash://system/** directory.

All directories defined in the *url* argument except the created one must exist.

Example 1. The following example creates a directory on FLASH:

```
switchxxxxxx# mkdir flash://date/aaa/
```

Example 2. The following example creates a directory on the mass-storage device connected to the USB port:

```
switchxxxxxx# mkdir usb://newdir/
```

more

To display the contents of a file, use the **more** command in User EXEC mode.

Syntax

more *url*

Parameters

- ***url***—Specifies the local URL or predefined file name of the file to display.

Command Mode

User EXEC mode

Example

The following example displays the running configuration file contents:

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

pwd

To show the current directory, use the **pwd** command in User EXEC mode.

Syntax

pwd [usb: I flash:]

Parameters

- **usb:**—Display the current directory on the USB driver.
- **flash:**—Display the current directory on the FLASH driver.

Command Mode

User EXEC mode

User Guidelines

Use the **pwd usb:** I **flash:** command to show the current directory on the specified driver.

Use the **pwd** command to show the current directory set by the recent **cd** command.

Example

The following example uses the **cd** command to change the current directory and then uses the **pwd** command to display that current directory:

```
switchxxxxxx> pwd
flash://
switchxxxxxx> cd date/aaa
switchxxxxxx> pwd
flash://date/aaa
```

reload

To reload the operating system, use the **reload** command in Privileged EXEC mode.

Syntax

reload [**in** [hhh:mm | mmm] | **at** hh:mm [day month]] | **cancel**]

reload cancel

Parameters

- **in** *hhh***:***mm* | *mmm*—Schedules a reload of the image 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 image 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 hours.
- ***day***—Number of the day in the range from 1 to 31.
- ***month***—Month of the year. (Range: Jan–Dec)
- **cancel**—Cancels a scheduled reload.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **reload** command to reload the switch.

Use the **reload** {**in** *hhh***:***mm* | *mmm* | **at** *hh***:***mm* [*day month*]} command the command to specify scheduled switch reload.

The **at** keyword can be configured only if the system clock has been set on the switch.

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.

Use the **reload cancel** command to cancel the scheduled reload.

Example 1. The following example reloads the switch:

```
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 image in 10 minutes:

```
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 image at 12:10 24 Aug:

```
switchxxxxxx# reload at 12:10 24 Aug
This command will reset the whole system and disconnect your current session. Reload is
scheduled for 12:10:00 UTC Sun Aug 24 2014 (in 1 hours and 12 minutes). Do you want to
continue ? (Y/N)[N]
```

Example 4. The following example reloads the image at 13:00:

```
switchxxxxxx# reload at 13:00 soft
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 5. The following example cancels a reload.

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

rename

To rename a local file or directory, use the **rename** command in Privileged EXEC mode.

Syntax

rename *url new-url*

Parameters

- *url*—Specifies the URL of the file or directory to be renamed. The predefined and network URLs cannot be configured.
- *new-url*—Specifies the new URL of the renamed file or directory. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

The *url* and *new-url* arguments must specifies the same driver.

The command cannot rename a network file or network directory.

The command cannot rename a file or directory into the **flash://system** directory.

Example 1. The following example renames the **flash://bin/text1.txt** file to **flash://archive/text1sav.txt**:

```
switchxxxxxx# cd flash://archive
switchxxxxxx# rename flash://bin/text1.txt ./text1sav.txt
```

Example 2. The following example renames the **flash://a/b** directory to the **flash://e/g/h** directory:

```
switchxxxxxx# pwd
flash://a/b/c/d
switchxxxxxx> dir flash://a
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://a
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
b                drw-        472148   Dec 13 2010 15:49:36
switchxxxxxx> dir flash://e/g/h
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://e/g/h
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
switchxxxxxx# rename flash://a/b flash://e/g/h
switchxxxxxx# pwd
flash://e/g/h/c/d
switchxxxxxx> dir flash://a
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://mng/
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
switchxxxxxx> dir flash://e/g/h
Permissions
  • d-directory
  • r-readable
  • w-writable
  • x-executable
134560K of 520000K are free
Directory of flash://e/g/h
File Name     Permission  File Size      Last Modified
---------     ----------  ---------   --------------------
c                drw-        720148   Dec 12 2010 17:49:36
```

rmdir

To remove a local directory, use the **rmdir** command in Privileged EXEC mode.

Syntax

rmdir *url*

Parameters

- *url*—Specifies the URL of the file or directory to be deleted. The predefined and network URLs cannot be configured.

Command Mode

Privileged EXEC mode

User Guidelines

Only empty directory can be deleted.

The command cannot remove a network directory.

The command cannot remove a directory into the **flash://system** directory.

Example 1. The following example removes the directory called ‘backup/config/’ from FLASH:

```
switchxxxxxx# rmdir flash://backup/config/
Remove flash://backup/config? [Y/N]Y
```

Example 2. The following example removes the directory called ‘aaa/config’ from the mass-storage device connected to the USB port:

```
switchxxxxxx# rmdir usb://aaa/config/
Remove directory usb://aaa/config? [Y/N]Y
```

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

This command has no arguments or keywords.

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 has not been modified for 24H).

When this service is disabled, the mirror-configuration file is deleted.

Example 1 - The following example disables the mirror-configuration service:

```
switchxxxxxx(config)# no service mirror-configuration
```

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

Example 2 - The following example enables the mirror-configuration service

```
switchxxxxxx(config)# service mirror-configuration
```

Service is enabled.

show bootvar / show version

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, use the **show bootvar** or **show version** command in User EXEC mode.

Syntax

show bootvar

show version

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

The **show bootvar** and **show version** commands have the same functionality.

Example 1. The following example gives an example of the command output after reload:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
```

```
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
  Version: 12.01
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Feb-2001
  Time: 11:13:17
```

Example 2. This example continues the inactive one, after applying the **boot system tftp://1.1.1.1/image_v14-01.ros** command:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
```

Example 3. This example continues the inactive one, after a system reload:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
Inactive-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
```

Example 4. This example continues the inactive one, after applying the **boot system inactive-image** command:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Inactive after reboot
Inactive-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Active after reboot
```

Example 5. This example continues the inactive one, after a system reload:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/_image_v12-03.ros
```

```
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
```

Example 7. The following example gives an example of the command output after applying the **boot system** command two times:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
  Version: 12.01
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Feb-2001
  Time: 11:13:17
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-01.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-04.ros
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-04.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
```

Example 8. The following example gives an example of the command output after applying the **boot system tftp://1.1.1.1/image_v14-01.ros** command and the **boot system inactive-image** command:

```
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v12-01.ros
  Version: 12.01
  MD5 Digest: 3FA000012857D8855AABC7577AB8999
  Date: 04-Feb-2001
  Time: 11:13:17
switchxxxxxx# boot system tftp://1.1.1.1/image_v14-01.ros
switchxxxxxx# show bootvar
```

```
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
  Inactive after reboot
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
  Active after reboot
switchxxxxxx# boot system inactive-image
switchxxxxxx# show bootvar
Active-image: flash://system/images/image_v12-03.ros
  Version: 12.03
  MD5 Digest: 63FA000012857D8855AABEA7451265456
  Date: 04-Jul-2014
  Time: 15:03:07
Inactive-image: flash://system/images/image_v14-01.ros
  Version: 14.01
  MD5 Digest: 23FA000012857D8855AABC7577AB5562
  Date: 24-Jul-2014
  Time: 23:11:17
```

show mirror-configuration service

To display the mirror-configuration service status, use the **show mirror-configuration service** command in User EXEC mode.

Syntax

show mirror-configuration service

Command Mode

User EXEC mode

Example

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

```
switchxxxxxx# show mirror-configuration service
Mirror-configuration service is enabled
```

show reload

To display the reload status on the switch, use the **show reload** command in User EXEC mode.

Syntax

show reload

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

You can use the **show reload** command to display a pending image reload.

Example 1. The following example displays information when scheduled reload has been configured:

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

Example 2. The following example displays information when scheduled reload has not been configured:

```
switchxxxxxx> show reload
No scheduled reload
```

show running-config

To display the contents of the currently running configuration file, use the **show running-config** command in Privileged EXEC mode.

show running-config [**interface** i***nterface-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 and certificates.
- **brief**—Displays configuration without SSL and SSH keys and certificates.

Default Configuration

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

Command Mode

Privileged EXEC mode

Example

The following example displays the running configuration file contents.

```
switchxxxxxx# show running-config
config-file-header
AA307-02
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
```

```
file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
unit-type unit 1 network te uplink none
unit-type unit 2 network te uplink none
unit-type unit 3 network te uplink none
unit-type unit 4 network te uplink none
unit-type-control-end
!
no spanning-tree
interface range gi1/0/1-4
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#
```

show startup-config

To display the Startup Configuration file contents, use the **show startup-config** command in Privileged EXEC mode.

Syntax

show startup-config [**interface** ***interface-id-list***]

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.

Command Mode

Privileged EXEC mode

Example

The following example displays the startup configuration file contents.

```
switchxxxxxx# show startup-config
config-file-header
AA307-02
v1.2.5.76 / R750_NIK_1_2_584_002
CLI v1.0
file SSD indicator encrypted
@
ssd-control-start
ssd config
```

```
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
no spanning-tree
interface range gi1/0/1-4
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#
```

show diff-config

-

write

To save the running configuration to the startup configuration file, use the **write** command in Privileged EXEC mode.

Syntax

write

write memory

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

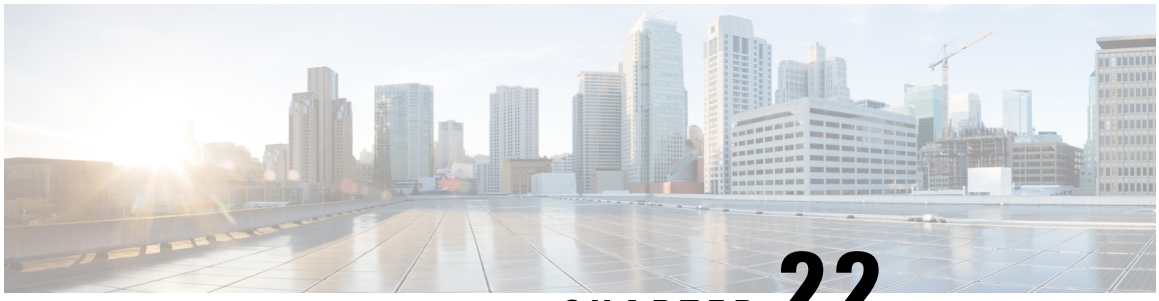
Use the **write** command or the **write memory** command to save the Running Configuration file into the Startup Configuration file.

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
```



CHAPTER 22

FIPS Commands

Note FIPS 140-2 Compliance is supported on firmware version 4.1.6.x and above.

- fips mode, on page 385
- show fips status, on page 386

fips mode

To set the device FIPS (Federal Information Processing Standards 140-2) operating mode after device reboot, use the fips mode command in Privileged EXEC mode.

Syntax

fips mode {disable | enable}

Parameters

- **disable** — Sets the device mode to FIPS non-compliant mode.
- **enable** — Sets the device mode to FIPS compliant mode.

Default Configuration

By default the device operates in FIPS non-compliant mode.

Command Mode

Privileged EXEC mode

User Guidelines

FIPS mode setting takes effect only after device reboot, and switching between FIPS modes will initiate a device reboot. When changing FIPS mode a confirmation message is displayed, informing the user that the change of FIPS mode will reboot the device and remove configuration related to SSH and HTTPS keys and certificates. Following the device reboot the user may need to reconfigure these settings.

If the device configuration includes unsaved settings, then the user will be prompted to save these changes.

Examples

Example 1. The following example sets the mode after device reload to FIPS compliant mode:

```
switchxxxxxx# fips mode enable
WARNING: Changing FIPS mode will reboot the device.
SSH keys, HTTPS keys, HTTPS certificates and trusted remote SSH server
fingerprints will be deleted.
In addition, SSH DSA key types will not be supported.
Do you wish to continue ? (Y/N)[N] Y
You haven't saved your changes. Are you sure you want to continue ? (Y/N)[N] Y
This command will reset the whole system and disconnect your current session.
Do you want to continue ? (Y/N)[N] Y
Shutting down ...
Shutting down ...
```

Example 2. The following example sets the mode after device reload to FIPS non-compliant mode:

```
switchxxxxxx# fip mode disable
WARNING: Changing FIPS mode will reboot the device.
SSH keys, HTTPS keys, HTTPS certificates and trusted remote SSH server
fingerprints will be deleted.
Do you wish to continue ? (Y/N)[N] Y
You haven't saved your changes. Are you sure you want to continue ? (Y/N)[N] Y
This command will reset the whole system and disconnect your current session.
Do you want to continue ? (Y/N)[N] Y
Shutting down ...
Shutting down ...
```

show fips status

To display if the device is operating in FIPS (Federal Information Processing Standards 140-2) compliant mode, use the show fips status command in Privileged EXEC mode.

Syntax

show fips status

Command Mode

Privileged EXEC mode

Examples

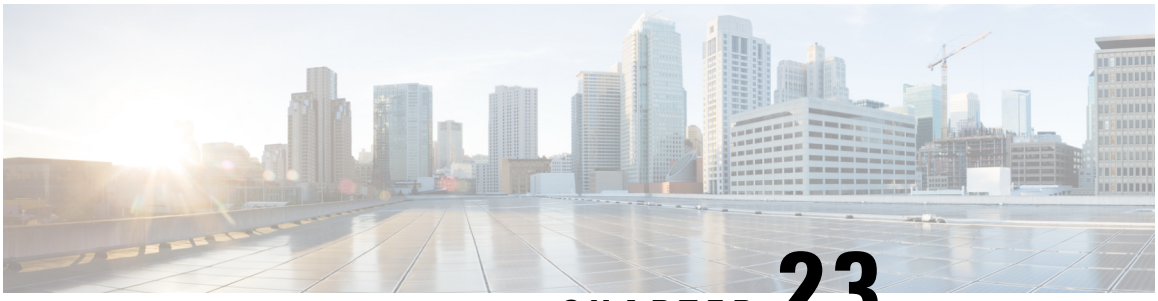
Example 1. The following example displays FIPS mode information when the device is operating in FIPS compliant mode:

```
switchxxxxxx# show fips status
FIPS mode: enabled
FIPS version: 140-2
Self-Tests: Passed
FIPS (Default) Library Context Providers:
name: OpenSSL Base Provider
version: 3.0.14
status: active
name: OpenSSL FIPS Provider
```

```
version: 3.0.9
status: active
```

Example 2. The following example displays FIPS mode information when the device is operating in FIPS non-compliant mode:

```
switchxxxxxx# show fips status
FIPS mode: disabled
Non-FIPS (Default) Library Context Providers:
name: OpenSSL Default Provider
version: 3.0.14
status: active
```



CHAPTER 23

GVRP Commands

This chapter contains the following sections:

- clear gvrp statistics, on page 389
- gvrp enable (Global), on page 390
- gvrp enable (Interface), on page 390
- gvrp registration-forbid, on page 391
- gvrp vlan-creation-forbid, on page 391
- show gvrp configuration, on page 392
- show gvrp error-statistics, on page 393
- show gvrp statistics, on page 393

clear gvrp statistics

To clear GVRP statistical information for all interfaces or for a specific interface, use the **clear gvrp statistics** Privileged EXEC mode command.

Syntax

clear gvrp statistics *[interface-id]*

Parameters

Interface-id—(Optional) 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 gi1/0/4.

```
switchxxxxxx#  clear gvrp statistics gi1/0/4
```

gvrp enable (Global)

To enable the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) globally, use the **gvrp enable** Global Configuration mode command. To disable GVRP on the device, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Parameters

This command has no arguments or keywords.

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
```

gvrp enable (Interface)

To enable GVRP on an interface, use the **gvrp enable** Interface (Ethernet, Port Channel) Configuration mode command. To disable GVRP on an interface, use the **no** form of this command.

Syntax

gvrp enable

no gvrp enable

Parameters

This command has no arguments or keywords.

Default Configuration

GVRP is disabled on all interfaces.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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 gi1/0/4.

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  gvrp enable
```

gvrp registration-forbid

To deregister all dynamic VLANs on a port and prevent VLAN creation or registration on the port, use the **gvrp registration-forbid** Interface Configuration mode command. To allow dynamic registration of VLANs on a port, use the **no** form of this command.

Syntax

gvrp registration-forbid

no gvrp registration-forbid

Parameters

This command has no arguments or keywords.

Default Configuration

Dynamic registration of VLANs on the port is allowed.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example forbids dynamic registration of VLANs on gi1/0/2.

```
switchxxxxxx(config-if)#  interface gi1/0/2
switchxxxxxx(config-if)#  gvrp registration-forbid
```

gvrp vlan-creation-forbid

To disable dynamic VLAN creation or modification, use the **gvrp vlan-creation-forbid** Interface Configuration mode command. To enable dynamic VLAN creation or modification, use the **no** form of this command.

Syntax

gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables dynamic VLAN creation on gi1/0/3.

```
switchxxxxxx(config-if)#  interface gi1/0/3
switchxxxxxx(config-if)#  gvrp vlan-creation-forbid
```

show gvrp configuration

To display GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation are enabled, and which ports are running GVRP, use the **show gvrp configuration** EXEC mode command.

Syntax

show gvrp configuration *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
- **detailed**—(Optional) 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

User 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
----    ----------- --------   -------------    ----   -----   ----------
gi1/0/1     Enabled     Forbidden   Disabled         600     200    10000
gi1/0/2     Enabled     Normal      Enabled          1200    400    20000
```

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—(Optional) 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

User 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
-------- ------- ------- ------- ------- --------
 gi1/0/1      0       0       0       0       0
 gi1/0/2      0       0       0       0       0
 gi1/0/3      0       0       0       0       0
 gi1/0/4      0       0       0       0       0
```

show gvrp statistics

To display GVRP statistics for all interfaces or for a specific interface, use the **show gvrp statistics** EXEC mode command.

Syntax

show gvrp statistics *[interface-id]*

Parameters

interface-id—(Optional) 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

User EXEC mode

Example

The following example displays GVRP statistical information.

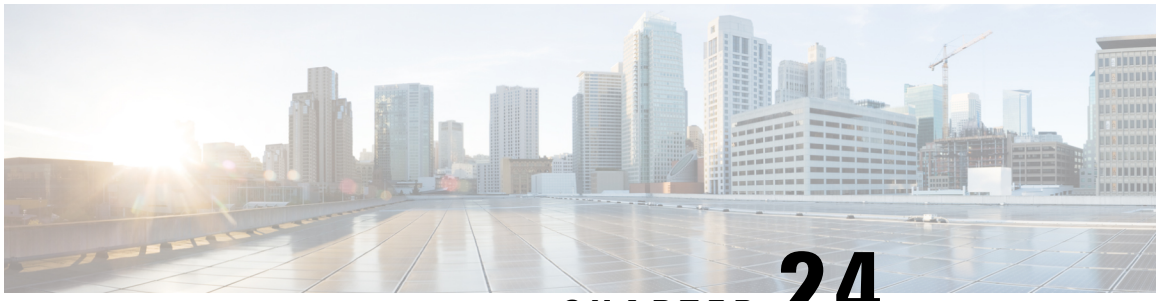
```
switchxxxxxx#  show gvrp statistics
```

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
-----	----	----	----	----	----	----	----	----	----	----	----	---
gi1/0/1	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/2	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/3	0	0	0	0	0	0	0	0	0	0	0	0
gi1/0/4	0	0	0	0	0	0	0	0	0	0	0	0



CHAPTER 24

Green Ethernet Commands

This chapter contains the following sections:

- green-ethernet energy-detect (global), on page 395
- green-ethernet energy-detect (interface), on page 396
- green-ethernet short-reach (global), on page 396
- green-ethernet short-reach (interface), on page 397
- green-ethernet power-meter reset, on page 398
- show green-ethernet, on page 398

green-ethernet energy-detect (global)

To enable Green-Ethernet Energy-Detect mode globally, use the **green-ethernet energy-detect** Global Configuration mode command. To disable this feature, use the **no** form of this command.

Syntax

green-ethernet energy-detect

no green-ethernet energy-detect

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)#  green-ethernet energy-detect
```

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

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Energy-Detect only works on copper ports. 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 gi1/0/1
switchxxxxxx(config-if)#  green-ethernet energy-detect
```

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

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)#  green-ethernet short-reach
```

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

This command has no arguments or keywords.

Default Configuration

Disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

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 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 gi1/0/1
switchxxxxxx(config-if)#  green-ethernet short-reach
```

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

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#  green-ethernet power-meter reset
```

show green-ethernet

To display green-ethernet configuration and information, use the **show green-ethernet** Privileged EXEC mode command.

Syntax

show green-ethernet [*interface-id* | ***detailed***]

Parameters

- **interface-id**—(Optional) Specifies an Ethernet port
- **detailed**—(Optional) 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 relevant to the power saved by:

- Port LEDs
- Energy detect
- Short reach

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.

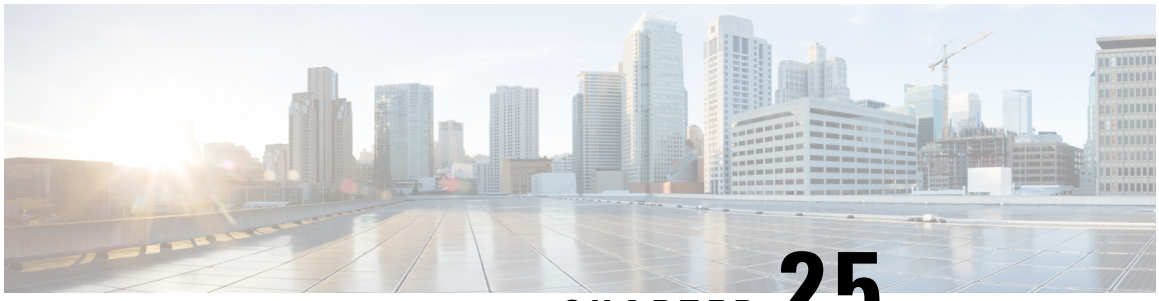
If there are a several reasons, then only the highest priority reason is displayed.

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 (10mbps,100mbps)
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
Disable Port LEDs mode: Enabled
Power Savings: 24% (1.08W out of maximum 4.33W)
Cumulative Energy Saved: 33 [Watt*Hour]
* Estimated Annual Power saving: 300 [Watt*Hour]
* Annual estimate is based on the saving during the previous week
NA - information for previous week is not available
Short-Reach cable length threshold: 50m
Port     Energy-Detect       Short-Reach           VCT Cable
      Admin Oper Reason   Admin Force Oper Reason   Length
----  ----- ---- -------  ----- ----- ---- -------  ------
gi1/0/1   on    on            off  off   off
gi1/0/2   on    off  LU       on   off   on          < 50
gi1/0/3   on    off  LU       off  off   off
```



CHAPTER 25

IGMP Commands

This chapter contains the following sections:

- clear ip igmp counters, on page 401
- ip igmp last-member-query-count, on page 402
- ip igmp last-member-query-interval, on page 402
- ip igmp query-interval, on page 403
- ip igmp query-max-response-time, on page 404
- ip igmp robustness, on page 405
- ip igmp version, on page 405
- show ip igmp counters, on page 406
- show ip igmp groups, on page 407
- show ip igmp groups summary, on page 408
- show ip igmp interface, on page 409

clear ip igmp counters

To clear the Internet 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***—(Optional) Interface Identifier

Command Mode

Privileged EXEC mode

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:

```
switchxxxxxx# clear ip igmp counters vlan 100
```

ip igmp last-member-query-count

To configure the Internet Group Management Protocol (IGMP) last member query counter, use the **ip igmp last-member-query-count** command in Interface Configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ip igmp last-member-query-count count

no ip igmp last-member-query-count

Parameters

count—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of IGMP Robustness variable.

Command Mode

Interface Configuration mode

User Guidelines

Use the **ip igmp robustness** command to change the IGMP last member query counter.

Example

The following example changes a value of the IGMP last member query counter to 3:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp last-member-query-count 3
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp last-member-query-interval 1500
switchxxxxxx(config-if)# exit
```

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 30 to 18000.

Default Configuration

The default IGMP query interval is 125 seconds.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp query-interval 180
switchxxxxxx(config-if)# exit
```

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 igmp query-max-response-time

Parameters

- ***seconds***—Maximum response time, in seconds, advertised in IGMP queries. (Range: 5–20)

Default Configuration

10 seconds.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp query-max-response-time 8
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip igmp robustness 3
switchxxxxxx(config-if)# exit
```

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

3

Command Mode

Interface Configuration mode

User Guidelines

Use the commnad to change the default version of IGMP>

Example

The following example configures the router to use IGMP Version 2:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp version 2
switchxxxxxx(config-if)# exit
```

show ip igmp counters

To display the Internet Group Management Protocol (IGMP) traffic counters, use the **show ip igmp counters** command in User EXEC mode.

Syntax

show ip igmp counters [*interface-id*]

Parameters

- ***interface-id***—(Optional) Interface Identifier.

Command Mode

User EXEC mode

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:

```
switchxxxxxx# 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
```

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 mode.

Syntax

show ip igmp groups [*group-name* | *group-address* | *interface-id*] [**detail**]

Parameters

- ***group-name* | *group-address***—(Optional) IP address or name of the multicast group.
- ***interface-id***—(Optional) Interface identifier.
- **detail**—(Optional) Displays detailed information about individual sources.

Command Mode

User EXEC mode

User Guidelines

Use the **show ip igmp groups** [**detail**] command to display all directly connected groups.

Use the **show ip igmp groups** [*group-name* | *group-address*] [**detail**] command to display one given directly connected group.

Use the **show ip igmp groups** *interface-id* [**detail**] command to display all groups directly connected to the given interface.

Example 1. The following is sample output from the **show ip igmp groups** command. It shows all of the groups joined by VLAN 100:

```
switchxxxxxx# 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:

```
switchxxxxxx# 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
```

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 mode.

Syntax

show ip igmp groups summary

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

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:

```
switchxxxxxx# show ip igmp groups summary
GMP 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.

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** command in User EXEC mode.

Syntax

show ip igmp interface [*interface-id*]

Parameters

- ***interface-id***—(Optional) Interface identifier.

Command Mode

User EXEC mode

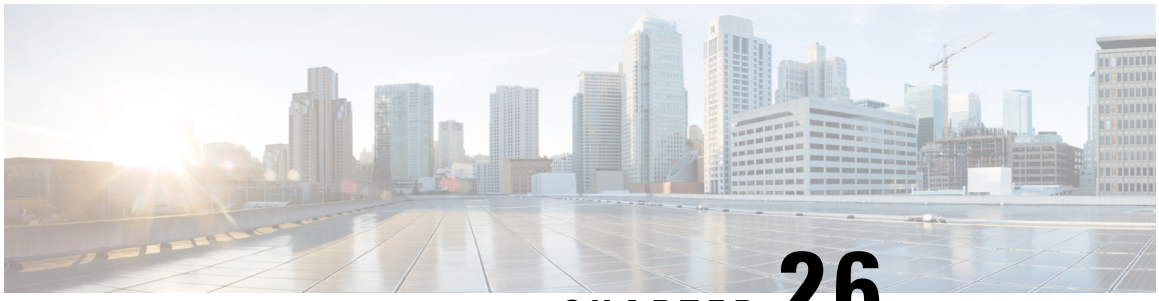
User Guidelines

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:

```
switchxxxxxx# 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
```



CHAPTER 26

IGMP Proxy Commands

This chapter contains the following sections:

- ip igmp-proxy, on page 411
- ip igmp-proxy downstream protected, on page 412
- ip igmp-proxy downstream protected interface, on page 413
- ip igmp-proxy ssm, on page 413
- show ip igmp-proxy interface, on page 414

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 mode

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 1. The following example adds a downstream interface to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip igmp-proxy vlan 200
switchxxxxxx(config-if)# exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface range vlan 100-105
switchxxxxxx(config-if)# ip igmp-proxy vlan 200
switchxxxxxx(config-if)# exit
```

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 ip 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:

```
switchxxxxxx(config)# ip igmp-proxy downstream protected
```

ip igmp-proxy downstream protected interface

To disable or enable forwarding of IP Multicast traffic from a given downstream interface, use the **ip igmp-proxy downstream protected interface** command in Interface Configuration mode. To return to default, use the **no** form of this command.

Syntax

ip igmp-proxy downstream protected interface {enabled | disabled}

no ip igmp-proxy downstream protected interface

Parameters

- **enabled**—Downstream interface protection on the interface is enabled. IPv4 Multicast traffic arriving on the interface will not be forwarded.
- **disabled**—Downstream interface protection on the interface is disabled. IPv4 Multicast traffic arriving on the interface will be forwarded.

Default Configuration

Global downstream protection configuration (see the **ip igmp-proxy downstream protected** command)

Command Mode

Interface Configuration mode

User Guidelines

Use the **ip igmp-proxy downstream protected interface disabled** command to block forwarding from the given downstream interface.

Use the **ip igmp-proxy downstream protected interface enabled** command to allow forwarding from the given downstream interface.

The command can be configured only for a downstream interface. When a downstream interface is removed from the IGMP Proxy tree the configuration is removed too.

Example

The following example prohibits forwarding from downstream interface vlan 100:

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ip igmp-proxy downstream protected interface enabled
switchxxxxxx(config-if)# exit
```

ip igmp-proxy ssm

To define the Source Specific Multicast (SSM) range of IP Multicast addresses, use the **ip igmp-proxy ssm** command in Global Configuration mode. To disable the SSM range, use the **no** form of this command.

Syntax

ip igmp-proxy ssm {**default** | **range** *access-list*}

no ip igmp-proxy ssm

Parameters

- **default**—Defines the SSM range access list to 232.0.0.0/8 (see rfc4607).
- **range** *access-list*—Specifies the standard IP access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global Configuration mode

User Guidelines

A new **ip igmp-proxy ssm** command overrides the previous **ip igmp-proxy ssm** command.

Use the **no ip igmp-proxy 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 list **list1**:

```
switchxxxxxx(config)# ip access-list list1 permit 224.2.151.0/24
switchxxxxxx(config)# ip access-list list1 deny 224.2.152.141
switchxxxxxx(config)# ip access-list list1 permit 224.2.152.0/24
switchxxxxxx(config)# ip igmp-proxy ssm range list1
```

show ip igmp-proxy interface

To display information about interfaces configured for IGMP Proxy, use the **show ip igmp-proxy interface** command in User EXEC mode or Privileged EXEC mode.

Syntax

show ip igmp-proxy interface [*interface-id*]

Parameters

- ***interface-id***—(Optional) Display IGMP Proxy information about the interface.

Command Mode

User EXEC mode

Privileged EXEC mode

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 1. The following example displays IGMP Proxy status on all interfaces where the IGMP Proxy is enabled:

```
switchxxxxxx# 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
Global Downdtream interfaces protection is disabled
SSM Access List Name:list1
Interface  Type         Interface Protection
 vlan 100  upstream
*vlan 102  downstream   enabled
*vlan 110  downstream   default
 vlan 113  downstream   disabled
```

Example 2. The following is sample output from the **show ip igmp-proxy interface** command for given upstream interface:

```
switchxxxxxx# show ip igmp-proxy interface vlan 100
```

* - the switch is the Querier on the interface

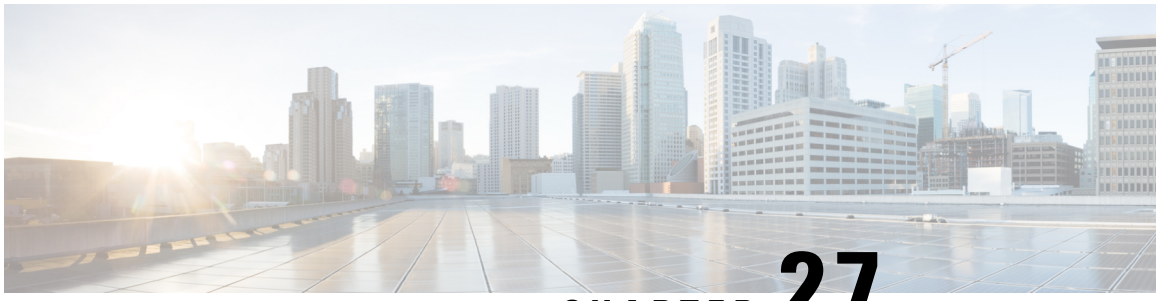
```
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name:
IP Multicast Tarffic Discarding from Downdtream interfaces is disabled
vlan 100 is a Upstream interface
Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the **show ip igmp-proxy interface** command for given downstream interface:

```
switchxxxxxx# show ip igmp-proxy interface vlan 102
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downdtream interfaces protection is disabled
vlan 102 is a Downstream interface
The switch is the Querier on vlan 102
Downsteam Interface protection is enabled
SSM Access List Name: default
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:

```
switchxxxxxx# show ip igmp-proxy interface vlan 1
IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is disabled
```



CHAPTER 27

IGMP Snooping Commands

This chapter contains the following sections:

- ip igmp snooping (Global), on page 417
- ip igmp snooping vlan, on page 418
- ip igmp snooping vlan mrouter, on page 418
- ip igmp snooping vlan mrouter interface, on page 419
- ip igmp snooping vlan forbidden mrouter, on page 420
- ip igmp snooping vlan static, on page 421
- ip igmp snooping vlan multicast-tv, on page 421
- ip igmp snooping map cpe vlan, on page 422
- ip igmp snooping querier, on page 423
- ip igmp snooping vlan querier, on page 424
- ip igmp snooping vlan querier address, on page 424
- ip igmp snooping vlan querier election, on page 425
- ip igmp snooping vlan querier version, on page 426
- ip igmp snooping vlan immediate-leave, on page 426
- ip igmp snooping map cpe vlan, on page 427
- show ip igmp snooping groups, on page 428
- show ip igmp snooping interface, on page 429
- show ip igmp snooping mrouter, on page 429
- show ip igmp snooping multicast-tv, on page 430

ip igmp snooping (Global)

To enable Internet Group Management Protocol (IGMP) snooping, use the **ip igmp snooping** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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
```

ip igmp snooping vlan

To enable IGMP snooping on a specific VLAN, use the **ip igmp snooping vlan** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Parameters

- ***vlan-id***—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

IGMP snooping can be enabled only on static VLANs.

IGMPv1, IGMPv2, and IGMPv3 Snooping are supported.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 2
```

ip igmp snooping vlan mrouter

To enable automatic learning of Multicast router ports on a VLAN, use the **ip igmp snooping vlan mrouter** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

no ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**

Parameters

- ***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
```

ip igmp snooping vlan mrouter interface

To define a port that is connected to a Multicast router port, use the **ip igmp snooping mrouter interface** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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-id***—Specifies the VLAN.
- ***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 gi1/0/1
```

ip igmp snooping vlan forbidden mrouter

To forbid a port from being defined as a Multicast router port by static configuration or by automatic learning, use the **ip igmp snooping vlan forbidden mrouter** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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-id***—Specifies the VLAN.
- ***interface-list***—Specifies a list of interfaces. The interfaces can be of 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 gi1/0/1
```

ip igmp snooping vlan static

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 **ip igmp snooping vlan static** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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-id***—Specifies the VLAN.
- ***ip-address***—Specifies the IP Multicast address.
- **interface** i*nterface-list*—(Optional) Specifies a list of interfaces. The interfaces can be of 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 gi1/0/1
```

ip igmp snooping vlan multicast-tv

To define the Multicast IP addresses that are associated with a Multicast TV VLAN, use the **ip igmp snooping vlan multicast-tv** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **multicast-tv** *first-ip-multicast-address* [*last-ip-multicast-address* | {**count** *number*}]

no ip igmp snooping vlan *vlan-id* **multicast-tv** *first-ip-multicast-address* [*last-ip-multicast-address* | {**count** *number*}]

Parameters

- ***vlan-id***—Specifies the VLAN
- ***first-ip-multicast-address***—The first Multicast IP address of the range
- ***last-ip-multicast-address***—The last Multicast IP address of the range
- **count** *number*—(Optional) Configures multiple contiguous Multicast IP addresses. If not specified, the default is 1.

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
```

ip igmp snooping map cpe vlan

To map CPE VLANs to Multicast-TV VLANs, use the **ip igmp snooping map cpe vlan** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping map cpe vlan *cpe-vlan-id* **multicast-tv vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

Parameters

- ***cpe-vlan-id***—Specifies the CPE VLAN ID.

- **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
```

ip igmp snooping querier

To enable globally the IGMP Snooping querier, use the **ip igmp snooping querier** command in Global Configuration mode. To disable the IGMP Snooping querier globally, use the **no** form of this command.

Syntax

ip igmp snooping querier

no ip igmp snooping querier

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

To run the IGMP Snooping querier on a VLAN, you have enable it globally and on the VLAN.

Example

The following example disables the IGMP Snooping querier globally:

```
switchxxxxxx(config)# no ip igmp snooping querier
```

ip igmp snooping vlan querier

To enable the IGMP Snooping querier on a specific VLAN, use the **ip igmp snooping vlan querier** command in Global Configuration mode. To disable the IGMP Snooping querier on the VLAN interface, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **querier**

no ip igmp snooping vlan *vlan-id* **querier**

Parameters

- ***vlan-id***—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The IGMP Snooping querier can be enabled on a VLAN only if IGMP Snooping is enabled for that VLAN.

Example

The following example enables the IGMP Snooping querier on VLAN 1:

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier
```

ip igmp snooping vlan querier address

To define the source IP address that the IGMP snooping querier uses, use the **ip igmp snooping vlan querier address** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **querier address** *ip-address*

no ip igmp snooping vlan *vlan-id* **querier address**

Parameters

- ***vlan-id***—Specifies the VLAN.
- ***ip-address***—Source IP address.

Default Configuration

If an IP address is configured for the VLAN, it is used as the source address of the IGMP snooping querier. If there are multiple IP addresses, the minimum IP address defined on the VLAN is used.

Command Mode

Global Configuration mode

User Guidelines

If an IP address is not configured by this command, and no IP address is configured for the querier's VLAN, the querier is disabled.

Example

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier address 10.5.234.205
```

ip igmp snooping vlan querier election

To enable IGMP Querier election mechanism of an IGMP Snooping querier on a specific VLAN, use the **ip igmp snooping vlan querier election** command in Global Configuration mode. To disable Querier election mechanism, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **querier election**

no ip igmp snooping vlan *vlan-id* **querier election**

Parameters

- ***vlan-id***—Specifies the VLAN.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

Use the **no** form of the **ip igmp snooping vlan querier election** command to disable IGMP Querier election mechanism on a VLAN. If the IGMP Querier election mechanism is enabled, the IGMP Snooping querier supports the standard IGMP Querier election mechanism specified in RFC2236 and RFC3376. If IGMP Querier election mechanism is disabled, IGMP Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier - it starts sending General Query messages. Once the switch acts as a Querier, it will stop sending General Query messages if it detects another Querier on the VLAN. In this case, the switch will

resume sending General Query messages if it does hear another Querier for Query Passive interval that equals to

<Robustness>*<Query Interval> + 0.5*<Query Response Interval).

It is recommended to disable IGMP Querier election mechanism if there is an IPM Multicast router on the VLAN.

Example

The following example disables IGMP Snooping Querier election on VLAN 1:

```
switchxxxxxx(config)# no ip igmp snooping vlan 1 querier election
```

ip igmp snooping vlan querier version

To configure the IGMP version of an IGMP Snooping querier on a specific VLAN, use the **ip igmp snooping vlan querier version** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **querier version** {**2** | **3**}

no ip igmp snooping vlan *vlan-id* **querier version**

Parameters

- ***vlan-id***—Specifies the VLAN.
- **querier version 2**—Specifies that the IGMP version would be IGMPv2.
- **querier version 3**—Specifies that the IGMP version would be IGMPv3.

Default Configuration

IGMPv2.

Command Mode

Global Configuration mode

Example

The following example sets the version of the IGMP Snooping Querier VLAN 1 to 3:

```
switchxxxxxx(config)# ip igmp snooping vlan 1 querier version 3
```

ip igmp snooping vlan immediate-leave

To enable the IGMP Snooping Immediate-Leave processing on a VLAN, use the **ip igmp snooping vlan immediate-leave** Global Configuration mode command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp 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

The following example enables IGMP snooping immediate-leave feature on VLAN 1.

```
switchxxxxxx(config)# ip igmp snooping vlan 1 immediate-leave
```

ip igmp snooping map cpe vlan

To map CPE VLANs to Multicast-TV VLANs, use the **ip igmp snooping map cpe vlan** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ip igmp snooping map cpe vlan *cpe-vlan-id* **multicast-tv vlan** *vlan-id*

no ip igmp snooping map cpe vlan *vlan-id*

Parameters

- ***cpe-vlan-id***—Specifies the CPE VLAN ID.
- **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
```

show ip igmp snooping groups

To display the Multicast groups learned by the IGMP snooping, use the **show ip igmp snooping groups** command in User EXEC mode.

Syntax

show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*] [**source** *ip-address*]

Parameters

- **vlan** *vlan-id*—(Optional) Specifies the VLAN ID.
- **ip-multicast-address** *ip-multicast-address*—(Optional) Specifies the IP multicast address.
- **ip-address** *ip-address*—(Optional) Specifies the IP source address.

Command Mode

User 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

Example

The following example shows sample output:

```
switchxxxxxx# show ip igmp snooping groups vlan 1
```

```
switchxxxxxx# show ip igmp snooping groups

Vlan  Group Address     Source Address  Include Ports  Exclude Ports  Comp-Mode
----  ----------------  --------------  -------------  -------------  ---------
1     239.255.255.250   *               gi1/0/1                       v2
```

show ip igmp snooping interface

To display the IGMP snooping configuration for a specific VLAN, use the **show ip igmp snooping interface** command in User EXEC mode.

Syntax

show ip igmp snooping interface *vlan-id*

Parameters

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

Command Mode

User 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
VLAN 1000
IGMP Snooping is enabled
IGMP snooping last immediate leave: enable
Automatic learning of Multicast router ports is enabled
IGMP Snooping Querier is enabled
IGMP Snooping Querier operation state: is not running
IGMP Snooping Querier version: 2
IGMP Snooping Querier election is enabled
IGMP Snooping Querier address: 194.12.10.166
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 interface active Querier address: 194.12.100.100 (remote)
Groups that are in IGMP version 1 compatibility mode:
231.2.2.3, 231.2.2.3
```

show ip igmp snooping mrouter

To display information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN, use the **show ip igmp snooping mrouter** command in User EXEC mode.

Syntax

show ip igmp snooping mrouter [**interface** *vlan-id*]

Parameters

- **interface** *vlan-id*—(Optional) Specifies the VLAN ID.

Command Mode

User 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	gi1/0/1	gi1/0/2	gi1/0/3-4

show ip igmp snooping multicast-tv

To display the IP addresses associated with Multicast TV VLANs, use the **show ip igmp snooping multicast-tv** EXEC mode command in User EXEC mode.

Syntax

show ip igmp snooping multicast-tv [**vlan** *vlan-id*]

Parameters

- **vlan** *vlan-id*—(Optional) Specifies the VLAN ID.

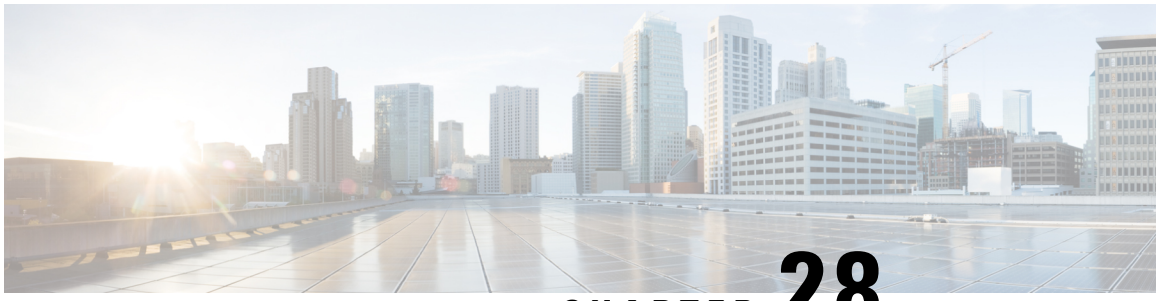
Command Mode

User EXEC mode

Example

The following example displays the IP addresses associated with all Multicast TV VLANs.

```
switchxxxxxx# show ip igmp snooping multicast-tv
VLAN First IP Address Last IP Address
---- ---------------- ---------------
1000 238.2.5.5 238.2.5.5
1000 239.255.0.0 239.255.1.1
1010 232.0.0.0 239.0.0.255
1010 239.0.1.2 239.255.4.5
```



CHAPTER 28

IP Addressing Commands

This chapter contains the following sections:

- ip address, on page 431
- ip address dhcp, on page 433
- renew dhcp, on page 433
- ip default-gateway, on page 434
- show ip interface, on page 435
- arp, on page 435
- arp timeout (Global), on page 436
- ip arp proxy disable, on page 437
- ip proxy-arp, on page 437
- clear arp-cache, on page 438
- show arp, on page 438
- show arp configuration, on page 439
- interface ip, on page 440
- ip helper-address, on page 440
- show ip helper-address, on page 441
- show ip dhcp client interface, on page 442

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

Bluetooth Interface

ip address *ip-address* {*mask* | */prefix-length*}

no ip address

In-Band interfaces:

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 (Ethernet, Port Channel, Bluetooth) Configuration mode

User Guidelines

Use the **ip address** command to define a static IP address on an interface.

In-Band interfaces

Multiple IP addresses are supported. A new defined IP address is added on the interface.

Defining a static IP address on an interface stops a DHCP client running on the interface and removes the IP address assigned by the DHCP client.

If a configured IP address overlaps another configured one a warning message is displayed. To change an existed IP address, delete the existed one and add the new one.

While no IP address is assigned either by DHCP client or manually the default IP address 192.168.1.254 is assigned on the Default VLAN.

Bluetooth interface

One IP address is supported. A new IP address defined on the Bluetooth interface overrides the previously defined IP address. The IP address configured on the Bluetooth interface cannot be on the same subnet as the addresses configured on the In-Band interfaces. The IP address on the Bluetooth interface does not support routing capabilities.

Example 1. 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
```

Example 2. The following example configures 3 overlapped IP addresses.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 1.1.1.1 255.0.0.0
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ip address 1.2.1.1 255.255.0.0
switchxxxxxx(config)# This IP address overlaps IP address 1.1.1.1/8 on vlan1, are you sure?
 [Y/N]Y
switchxxxxxx(config)# exit
switchxxxxxx(config)# interface vlan 3
switchxxxxxx(config-if)# ip address 1.3.1.1 255.255.0.0
switchxxxxxx(config)# This IP address overlaps IP address 1.1.1.1/8 on vlan1, are you sure?
```

```
 [Y/N]Y
switchxxxxxx(config)# exit
```

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

Command Mode

Interface Configuration mode

User Guidelines

Use the **ip address dhcp** command to enable DHCP client on the interface.

The **ip address dhcp** command removes all the manually configured addresses on the interface.

The default route (Default Gateway) received in DHCP Router option (Option 3) is assigned a metric of 8 for an In-Band interface and 6 for OOB.

Use the **no** form of the command to disable DHCP client on interface.

Example

The following example acquires an IP address for VLAN 100 from DHCP.

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ip address dhcp
```

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***—Specifies an interface.
- **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

Use the **renew dhcp** command to renew a DHCP address on an interface.

This command does not enable DHCP client on an interface and if DHCP client is not enabled on the interface, the command returns an error message.

Example

The following example renews an IP address on VLAN 19 that was acquired from a DHCP server:

```
switchxxxxxx# renew dhcp vlan 19
```

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 [***ip-address***]

Parameters

- ***ip-address***—Specifies the default gateway IP address.

Command Mode

Global Configuration mode

Default Configuration

No default gateway is defined.

User Guidelines

Use the **ip default-gateway** command to defines a default gateway (default route).

The **ip default-gateway** command adds the default route with metric of 4 for the gateway connected on an In-Band interface and 2 for the gateway connected on OOB.

Use the **no ip default-gateway** *ip-address* command to delete one default gateway.

Use the **no ip default-gateway** command to delete all default gateways.

Example

The following example defines default gateway 192.168.1.1.

```
switchxxxxxx(config)# ip default-gateway 192.168.1.1
```

show ip interface

Use the **show ip interface** EXEC mode command to display the usability status of configured IP interfaces.

Syntax

show ip interface [i*nterface-id***]**

Parameters

- ***interface-id***—Specifies an interface ID on which IP addresses are defined.

Default Configuration

All IP addresses.

Command Mode

User EXEC mode

Example 1 - The following example displays all configured IP addresses and their types:

```
switchxxxxxx# show ip interface

IP Address       I/F     I/F Status  Type   Directed   Redirect  Status
                          admin/oper        Broadcast
-------------    ------  ----------- ------- --------  --------- -----
10.5.230.232/24  vlan 1  UP/UP       Static  disable   Enabled   Valid
10.5.234.202/24 vlan 4 UP/DOWN Static disable Disabled Valid
10.5.240.200/24 oob UP/UP Static Valid
```

Example 2 - The following example displays the IP addresses configured on the given L2 interfaces and their types:

```
switchxxxxxx# show ip interface vlan 1

IP Address       I/F     I/F Status  Type   Directed   Redirect  Status
                          admin/oper        Broadcast
-------------    ------  ----------- ------- --------  --------- -----
10.5.230.232/24  vlan 1  UP/UP       Static  disable   Enabled   Valid
```

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.

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 vlan100
```

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, if IP Routing is enabled, and 300 seconds if IP Routing is disabled.

Command Mode

Global Configuration mode

Example

The following example configures the ARP timeout to 12000 seconds.

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

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

Default

Disabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command overrides any proxy ARP interface configuration.

The command is supported only when IP Routing is enabled.

Example

The following example globally disables ARP proxy.

```
switchxxxxxx(config)# ip arp proxy disable
```

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 enabled.

Command Mode

Interface Configuration mode

User Guidelines

This configuration can be applied only if at least one IP address is defined on a specific interface.

The command is supported only when IP Routing is enabled.

Example

The following example enables ARP proxy when the switch is in router mode.

```
switchxxxxxx(config-if)# ip proxy-arp
```

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
```

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.

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    gi1/0/1             10.7.1.102    00:10:B5:04:DB:4B    Dynamic
VLAN 1    gi1/0/2             10.7.1.135    00:50:22:00:2A:A4    Static
VLAN 2    gi1/0/1             11.7.1.135    00:12:22:00:2A:A4    Dynamic
          gi1/0/2             12.10.1.13    00:11:55:04:DB:4B    Dynamic
```

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:
VLAN 1:
 ARP Proxy: disabled
 ARP timeout:60000 Seconds
VLAN 10:
 ARP Proxy: enabled
 ARP timeout: 70000 Seconds
VLAN 20:
 ARP Proxy: enabled
 ARP timeout: 80000 Second (Global)
```

interface ip

Use the **interface ip** Global Configuration mode command to enter the IP Interface Configuration mode.

Syntax

interface ip *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)#
```

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: 1–59999). 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.

The *ip-interface* argument cannot be the OOB port.

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
```

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

User Guidelines

Example

The following example displays the IP helper addresses configuration on the system:

```
switchxxxxxx# show ip
```

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

show ip dhcp client interface

Use the **show ip dhcp client interface** command in User EXEC or Privileged EXEC mode to display DHCP client interface information.

Syntax

show ip dhcp client interface [*interface-id*]

Parameters

- ***interface-id***—Interface identifier.

Command Mode

User EXEC mode

User Guidelines

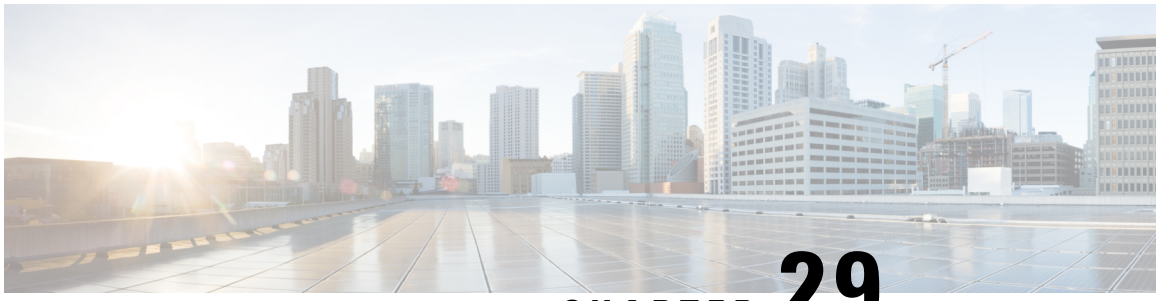
If no interfaces are specified, all interfaces on which DHCP client is enabled are displayed. If an interface is specified, only information about the specified interface is displayed.

Example

The following is sample output of the **show ip dhcp client interface** command:

```
switchxxxxxx# show ip dhcp client interface
VLAN 100 is in client mode
Address: 170.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
Default Gateway: 170.10.100.1
DNS Servers: 115.1.1.1, 87.12.34.20
DNS Domain Search List: company.com
Host Name: switch_floor7
Configuration Server Addresses: 192.1.1.1 202.1.1.1
Configuration Path Name: qqq/config/aaa_config.dat
Image Path Name: qqq/image/aaa_image.ros
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
VLAN 1200 is in client mode
Address: 180.10.100.100 Mask: 255.255.255.0 T1 120, T2 192
Default Gateway: 180.10.100.1
DNS Servers: 115.1.1.1, 87.12.34.20
DNS Domain Search List: company.com
```

```
Host Name: switch_floor7
Configuration Server Addresses: configuration.company.com
Configuration Path Name: qqq/config/aaa_config.dat
Image Path Name: qqq/image/aaa_image.ros
POSIX Timezone string: EST5EDT4,M3.2.0/02:00,M11.1.0/02:00
Option 43: 5A1N;K4;B3;IFE80::2E0:81FF:FE2D:3799;J6088
```



CHAPTER 29

IP Device Tracking Commands

•
• clear ip device tracking, on page 445
• ip device tracking probe auto-source, on page 446
• ip device tracking probe count (global), on page 447
• ip device tracking probe interval global, on page 448
• ip device tracking probe delay, on page 448
• ip device tracking probe count (interface), on page 449
• ip device tracking probe interval (interface), on page 450
• ip device tracking maximum, on page 451
• show ip device tracking, on page 451

clear ip device tracking

To clear IP Device Tracking table entries, use the clear ip device tracking command inPrivileged EXEC mode.

Syntax

clear ip device tracking {all | interface *interface-id* | **ip** *ip-address*| **mac** *mac-address*}

Parameters

- **all** — Clears all of the entries.
- **interface** *interface-id*— Clears the entries of the specified interface.
- **ip** *ip-address*— Clears a specific entry based on the provided IP address.
- **mac** *mac-address*— Clears a specific entry based on the provided MAC address.

Command Mode

Privileged EXEC mode

Examples

Example 1. The following example clears all of the IP Device Tracking entries:

```
switchxxxxxx# clear ip device tracking all
```

Example 2. The following example clears the IP Device Tracking entries learned on interface gi1:

```
switchxxxxxx# clear ip device tracking interface gi1
```

ip device tracking probe auto-source

To define the source IP used in ARP probes sent on VLANs without an IP address, use the ip device tracking probe auto-source command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking probe auto-source fallback host-ip mask override

no ip device tracking probe auto-source

Parameters

- *host-ip*—the Ip address to be used as the source IP in probes sent on VLANs without an IP address.
- *mask*—a mask, in IPv4 address format. This mask is applied to the host-ip parameter to determine the actual source IP to use on each VLAN.

Default Configuration

0.0.0.0 is used as the source IP address for probes that are sent on VLAN interfaces without an IP address.

Command Mode

Global Configuration mode

User Guidelines

ARP Probes sent by Layer 3 interfaces use the Interface's IP address as the source IP address for ARP probes sent by IP device tracking mechanism. This includes IP addresses configured on physical interfaces, Port-channels or VLANs

By default, the source IP address of ARP probes sent by a Layer 2 VLAN (a VLAN not configured with an IP address) is 0.0.0.0.

Use the ip device tracking probe auto-source command to change the source address used by L2 VLANs. The host-ip parameter defines the IP address to use as the ARP Probe source IP address. The mask parameter defines which bits in the host-ip parameter should be used as the ARP probe source IP, where 1 indicates "don't use" (or masked) and 0 indicates "use". The mask part of the IP address is taken from the IP address of the endpoint to which the ARP probe is sent. The mask must be contiguous from the high order bit (e.g 255.255.0.0 is a valid mask while 0.0.255.255 is not a valid mask)

Here are a few examples, where the ARP probe needs to be sent to 2 hosts: 10.10.1.100 and 20.1.1.100. The address segment taken from the host IP is highlighted:

- When the following command was specified: ip device tracking probe auto-source fallback 0.0.0.1 255.255.255.0 override:

- The source IP address used in the ARP probe sent to host 10.10.1.100 will be – 10.10.1.1
- The source IP address used in the ARP probe sent to host 20.1.1.100 will be – 20.1.1.1

- When the following command was specified: ip device tracking probe auto-source fallback 0.0.2.1 255.255.0.0 override:
  - The source IP address used in the ARP probe sent to host 10.10.1.100 will be – 10.10.2.1
  - The source IP address used in the ARP probe sent to host 20.1.1.100 will be – 20.1.2.1
  - 20.1.1.1

- When the following command was specified: ip device tracking probe auto-source fallback 0.3.2.1 255.0.0.0 override
  - The source IP address used in the ARP probe sent to host 10.10.1.100 will be – 10.3.2.1
  - The source IP address used in the ARP probe sent to host 20.1.1.100 will be – 20.3.2.1

Examples

The following example specifies that the probe source IP address will use the first 3 bytes of the network address and the value of 11 for the host segment (last byte):

```
switchxxxxxx(config)# ip device tracking probe auto-source fallback 0.0.0.11
255.255.255.0 override
```

ip device tracking probe count (global)

To define the global value of the number of ARP probes sent before removing an entry from the IP Device Tracking table, use the ip device tracking probe count command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking probe count count

no ip device tracking probe count

Parameters

- *count*—the number of ARP probes sent before removing an entry from IP Device Tracking table (range: 1-255).

Default Configuration

3 probes

Command Mode

Global Configuration mode

User Guidelines

The global count value is used on interfaces that were not configured with an interface level count value.

Examples

The following example specifies 5 probes as the global probe count:

```
switchxxxxxx(config)# ip device tracking probe count 5
```

ip device tracking probe interval global

To define the global value of the interval between ARP probes sent by the device, use the ip device tracking probe interval command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking probe interval *interval*

no ip device tracking probe interval

Parameters

- *interval*—the interval, in seconds, between ARP probes send by the device (range: 30-1814400 seconds).

Default Configuration

30 seconds

Command Mode

Global Configuration mode

User Guidelines

The global count value is used on interfaces that were not configured with an interface level interval value.

Examples

The following example specifies 35 seconds as the global probe interval:

```
switchxxxxxx(config)# ip device tracking probe interval 35
```

ip device tracking probe delay

To define the delay before sending an ARP probe to an in-active IP Device Tracking table entry, use the ip device tracking probe delay command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking probe delay *delay*

no ip device tracking probe delay

Parameters

- *delay*—the delay, in seconds, before the device sends an ARP probe to an inactive entry (range: 1-120 seconds).

Default Configuration

By default there is no delay when sending a probe to an in-active entry.

Command Mode

Global Configuration mode

User Guidelines

Configure a probe delay value in order to prevent a false duplicate address detection for an in-active entry. The probe delay defines the number of seconds the to wait before sending an ARP Probe to an in-active host. If the in-active host sends an ARP before the probe delay time expired then the device will wait for the probe interval before sending the next probe.

The probe-delay setting only affects probe sent for in-active entries. It does not effect probe count or interval used for verifying the existence of an existing hosts.

Examples

The following example defines a probe delay of 10 seconds:

```
switchxxxxxx(config)# ip device tracking probe delay 10
```

ip device tracking probe count (interface)

To define a specific ARP probe count value for an interface, use the ip device tracking probe count command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking probe count *count*

no ip device tracking probe count

Parameters

- *count*—the number of ARP probes sent before removing an entry from IP Device Tracking table (range: 1-255).

Default Configuration

The default count value for an interface is the global count value.

Command Mode

Interface Configuration mode(Ethernet, Port-Channel).

User Guidelines

Use this command on an interfaces to specify a count value for the interface that is different from the global count value. The global count value is 3 by default, or the value specified using the ip device tracking probe count (global) global mode command.

Examples

The following example specifies 7 probes as the probe count for interface gi1:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ip device tracking probe count 7
```

ip device tracking probe interval (interface)

To define a specific ARP probe interval value for an interface, use the ip device tracking probe interval command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking probe interval *interval*

no ip device tracking probe interval

Parameters

- *interval*—the interval, in seconds, between ARP probes send by the device (range: 30-1814400 seconds).

Default Configuration

The default interval value for an interface is the global interval value.

Command Mode

Interface Configuration mode

User Guidelines

Use this command on an interface to specify an interval value that is different from the global interval value. The global interval value is 30 seconds by default, or the value specified using the ip device tracking probe interval (global) global mode command.

Examples

The following example specifies an interval of 50 seconds between probes for interface gi1:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ip device tracking probe interval 50
```

ip device tracking maximum

To define the maximum number of IP Device Tracking entries that can be learned on an interface, use the ip device tracking maximum command in Interface Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ip device tracking maximum *max-device*

no ip device tracking maximum

Parameters

- *max-device* —the maximum number of devices that are connected to this interface that can be added as entries to the IP Device Tracking table (range: 0-65534 devices).

Default Configuration

By default the number of devices that can be learned on the interface is 65,535.

Command Mode

Interface Configuration mode

User Guidelines

Use this command to define the number of connected devices that can be added to the IP Device tracking table. The configurable range of the command is 0-65,534 devices. To allow learning 65,535 devices (the default) use the no form of the command.

Configuring a max-device value between 1-65,534 will enable the IP device Tracking feature on the interface. Configuring a max-device value of 0 will disable the feature on the interface. If the max-device value is set to the default value (65,535) then the feature will be enabled on the feature if 802.1x port-control is set to auto on the interface (command: dot1x port-control)

Examples

The following example specifies an interval of 50 seconds between probes for interface gi1:

```
switchxxxxxx(config)# interface gi1
switchxxxxxx(config-if)# ip device tracking probe interval 50
```

show ip device tracking

To display IP Device Tracking settings and table entries, use the show ip device tracking command in Privileged EXEC mode.

Syntax

show ip device tracking {all | interface *interface-id* | **ip** *ip-address*| **mac** *mac-address*}

Parameters

- **all** — Displays global settings and the entire IP Device Tracking table.
- **interface** *interface-id*— Displays the IP Device Tracking setting of the specified interface and the entries that were learned on this interface.
- **ip** *ip-address*— Displays the global level settings and a specific entry based on the provided IP address.
- **mac** *mac-address*— Displays the global level settings and a specific entry based on the provided MAC address.

Command Mode

Privileged EXEC mode

Examples

Example 1. The following example displays IP Device Tracking global settings and all of the table entries:

```
switchxxxxxx# show ip device tracking all
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 5
Global IP Device Tracking Probe Interval = 35
Global IP Device Tracking Probe Delay Interval = 0
IP Device Tracking Probe Auto Source = Disabled
IP Address MAC Address Vlan Interface Probe-Timeout State Source
----------- -------------- ---- ------- --------- ------ -----
10.2.13.10 68:05:ca:21:28:e6 13 gi1 30 Active arp
10.2.14.20 68:05:ca:21:28:d5 14 gi2 30 Active arp
Total number interfaces enabled: 2
Enabled interfaces:
gi1, gi2
```

Example 2. The following example displays the IP Device Tracking settings and entries for interface gi1:

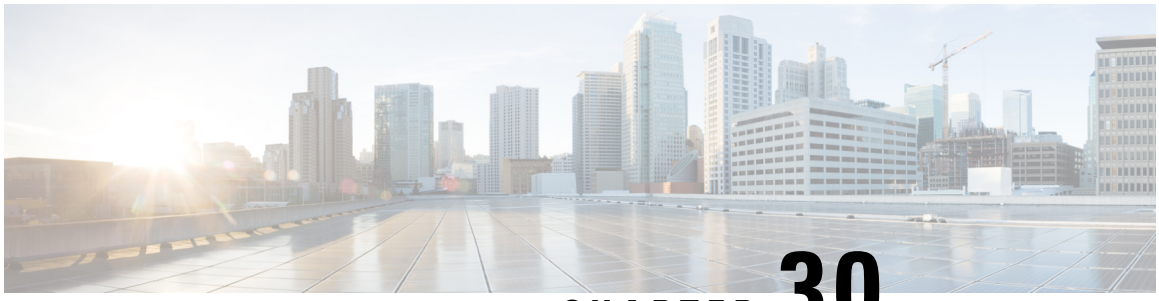
```
switchxxxxxx# show ip device tracking interface gi1
Interface gi1 is: STAND ALONE
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3 (Global)
IP Device Tracking Probe Interval = 30 (Global)
IP Device Tracking Enabled Features:
HOST_TRACK_CLIENT_SM
IP Address MAC Address Vlan Interface Probe-Timeout State Source
----------- -------------- ---- ------- --------- ------ -----
10.2.13.10 68:05:ca:21:28:e6 13 gi1 30 Active arp
```

Example 3. The following example displays a single IP Device Tracking entry. The entry is identified using the entry's IP address.

```
switchxxxxxx# show ip device tracking ip 10.2.14.20
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 5
Global IP Device Tracking Probe Interval = 35
Global IP Device Tracking Probe Delay Interval = 0
IP Address MAC Address Vlan Interface Probe-Timeout State Source
----------- -------------- ---- ------- --------- ------ -----
10.2.14.20 68:05:ca:21:28:d5 14 gi2 30 Active arp
Total number interfaces enabled: 2
Enabled interfaces:
gi1, gi2
```

Example 4. The following example displays a single IP Device Tracking entry. The entry is identified using the entry's MAC address.

```
switchxxxxxx# show ip device tracking mac 68:05:ca:21:28:d5
Global IP Device Tracking for clients = Enabled
Global IP Device Tracking Probe Count = 5
Global IP Device Tracking Probe Interval = 35
Global IP Device Tracking Probe Delay Interval = 0
IP Address MAC Address Vlan Interface Probe-Timeout State Source
---------- -------------- ---- ------- --------- ------ -----
10.2.14.20 68:05:ca:21:28:d5 14 gi2 30 Active arp
Total number interfaces enabled: 2
Enabled interfaces:
gi1, gi2
```



CHAPTER 30

IP Routing Protocol-Independent Commands

This chapter contains the following sections:

- accept-lifetime, on page 455
- cryptographic-algorithm, on page 457
- directed-broadcast, on page 458
- ip policy route-map, on page 459
- ip redirects, on page 460
- ip route, on page 461
- ip routing, on page 462
- key-string, on page 463
- key (key chain), on page 464
- key chain, on page 465
- send-lifetime, on page 466
- show ip protocols, on page 467
- show ip route, on page 468
- show ip route summary, on page 472
- show key chain, on page 472

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-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 acceptable year range is 2020-2037, with default start time and the earliest acceptable date is January 1 of the first acceptable year.

- **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 mode

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:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)#  ip rip authentication key-chain keychain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain keychain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string string1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string string2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
```

cryptographic-algorithm

To set a cryptographic algorithm to apply when using the key string configured for the key ID, use the cryptographic-algorithm command in Key Chain Key Configuration mode. To disable the cryptographic algorithm for the key ID, use the no form of this command.

Syntax

cryptographic-algorithm {md5 | hmac-sha-1 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512}

no cryptographic-algorithm

Parameters

- **md5**— Use MD5 as the cryptographic algorithm.
- **hmac-sha-1**— Use HMAC-SHA-1 as the cryptographic algorithm.
- **hmac-sha-256**— Use HMAC-SHA-256 as the cryptographic algorithm.
- **hmac-sha-384**— Use HMAC-SHA-384 as the cryptographic algorithm.
- **hmac-sha-512**— Use HMAC-SHA-512 as the cryptographic algorithm.

Default Configuration

The cryptographic algorithm is not set by default.

Command Mode

Key Chain Key Configuration mode

User Guidelines

Configuring the cryptographic-algorithm command defines the algorithm to use for each key in the key-chain. The same algorithm must be configured for the same key ID on the link partner interface.

Configuring a cryptographic algorithm for a key is mandatory for OSPF key-chain based authentication (command ip ospf authentication with key-chain option). If a key-chain used for OSPF authentication includes a key-id not configured with a cryptographic algorithm, then:

- If this is the only key in the key-chain, then OSPF packets are not sent on the IP interface and OSPF packets received on the IP interface are dropped.
- If the key-chain includes additional keys then only the keys configured with a cryptographic algorithm will be used. If a certain time-range (commands accept-lifetime or send-lifetime) is covered only by the key without a cryptographic algorithm, then during this time-range OSPF packets are not sent on the IP interface and OSPF packets received on the IP interface are dropped.

RIP key-chain based authentication (command ip rip authentication key-chain) supports only MD5 authentication. Therefore:

- If a "cryptographic-algorithm" was not configured for a key, then RIP authentication will use the specified key using the MD5 algorithm.
- If a "cryptographic-algorithm" was used to configure MD5 algorithm for a key, then RIP authentication will use the specified key using the MD5 algorithm.
- If a "cryptographic-algorithm" was used to configure any other (non MD5) algorithm for a key, then the key will not be used for RIP authentication.

Example

The following example configures a key chain called keychain1, with a key named string1.

The cryptographic algorithm is set to hmac-sha-256:

```
switchxxxxxx(config)# key chain keychain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string string1
switchxxxxxx(config-keychain-key)# cryptographic-algorithm hmac-sha-256
switchxxxxxx(config-keychain-key)# exit
```

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 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
```

ip policy route-map

To enable policy routing on an interface and identify a route map, use the **ip policy route-map** command in Interface Configuration mode. To disable policy routing, use the **no** form of this command.

Syntax

ip policy route-map *map-tag*

no ip policy route-map

Parameters

- ***map-tag***—Name of the route map to use for policy routing.

Default Configuration

No policy routing occurs on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the **ip policy route-map** command to enable policy routing on an interface. The actual policy routing will take a place if an IP address is defined on the interface.

The IP packets matched to the route-map conditions specified by the route map with the *map-tag* name will take a route depended on the action of the matched ACL:

- **permit**—The route specified by the set command Policy routing.
- **deny**—The route specified by the IP Forwarding table (regular routing).
- Name of the route map to use for policy routing.

The IP packets that are not matched, will be forwarded using the obvious shortest path.

IP policy routing on a Layer 2 interface is performed only when IP interface is defined, its status is UP, and the next hop is reachable. If the IP policy routing is not applied then the matched IP packets will be forwarded using the obvious shortest path.

Note. Of course, like in the case of regular IP Routing Policy Based IP Router routes only MAC "tome" IP frames. IP policy routing cannot be configured on an interface together with the following features:

- VLAN ACL

Example

The following example shows how to configure policy routing:

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# ip access-list extended pr-acl2
switchxxxxxx(config-ip-al)# permit tcp any any 156.122.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr 10
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# route-map pbr 20
switchxxxxxx(config-route-map)# match ip address access-list pr-acl2
switchxxxxxx(config-route-map)# set ip next-hop 50.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

ip redirects

Use the **ip redirects** command in IP Interface Configuration mode to enable the sending of ICMP 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

ip redirects

no ip redirects

Default Configuration

The sending of ICMP redirect messages is enabled.

Command Mode

IP Configuration mode

Example

The following example disables the sending of ICMP redirect messages on IP interface 1.1.1.1 and re-enables the messages on IP interface 2.2.2.2:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no ip redirects
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 2.2.2.2
switchxxxxxx(config-ip)# ip redirects
switchxxxxxx(config-ip)# exit
```

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** *value*]} | **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.
- **metric** *value*—Metric of the route. The default metric is 4 for the Next Hop on an In-Band interface and 2 for the Next Hop on OOB. Range: 1–255.
- **reject-route**—Stopping routing to the destination network.

Default Configuration

No static routes are established.

Command Mode

Global Configuration mode

User Guidelines

Use the **no ip route** command without the i*p-address* parameter to remove all static routes to the given subnet.

Use the **no ip route** command with the *ip-address* parameter to remove only one static route to the given subnet via the given next hop.

Example 1—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
switchxxxxxx(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

Example 2—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length :

```
switchxxxxxx(config)# ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

Example 3—The following example shows how to reject packets for network 194.1.1.0:

```
switchxxxxxx(config)# ip route 194.1.1.0 255.255.255.0 reject-route
```

Example 4—The following example shows how to remove all static routes to network 194.1.1.0/24:

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24
```

Example 5—The following example shows how to remove one static route to network 194.1.1.0/24 via 1.1.1.1:

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24 1.1.1.1
```

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 enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the command to enable IP Routing.

The switch supports one IPv4 stack on in-band interfaces and the OOB port.

The IP stack is always running on the OOB port as an IP host regardless whether IP routing is enabled.

The switch blocks routing between in-band interfaces and the OOB interface.

In the case when there are two best routes - one via an in-band and one via the OOB port, the switch will use the route via the OOB port.

DHCP Relay and IP Helper cannot be enabled on the OOB port.

Routing protocols cannot be enabled on the OOB port.

The IP subnet defined on the OOB port is not redistributed to routing protocols running on in-band interfaces.

Example The following example enables IP routing

```
switchxxxxxx(config)# ip routing
```

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 mode

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# version 2
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# exit
```

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:

```
switchxxxxxx(config)# key 1
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
```

```
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

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 *name-of-chain*

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:

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
```

```
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

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 mode

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:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
```

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 mode

Privileged EXEC mode

User Guidelines

The information displayed by the **show ip protocols** command is useful in debugging routing operations.

Example 1. The following is sample output from the **show ip protocols** command, showing active routing protocols:

```
switchxxxxxx# 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
```

Example 2. The following is sample output from the **show ip protocols** command with the **summary** keyword:

```
switchxxxxxx# show ipv6 protocols summary
IP Routing Protocol is "rip"
```

show ip route

To 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 [**address** *ip-address* {*mask* [**longer-prefixes**]} [*protocol* | **static** | **rejected** | **icmp | connected**]

Parameters

- **address** *ip-address*—IP address about which routing information should be displayed.
- ***mask***—The value of the subnet mask.
- **longer-prefixes**—Specifies that only routes matching the IP address and mask pair should be displayed.
- ***protocol***—The name of the origin of the protocol to be displayed. Use one of the following arguments:
- **rip**—Displays routes added by RIP
- **connected**—Displays connected routes.

- **icmp**—Displays routes added by ICMP Direct.
- **rejected**—Displays rejected routes.
- **static**—Displays static routes.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use this command without parameters to display the whole IPv6 Routing table.

Use this command with parameters to specify required routes.

Example 1. The following is sample output from the **show ip route** command when IP Routing is not enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)IP Forwarding: disabled
Codes: > - best, C - connected, S - static, I - ICMP
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 1/2 10.119.254.244 00:02:22 vlan2
S> 10.10.0.0/16 1/1 10.120.254.244 00:02:22 vlan3
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

Example 2. The following is sample output from the **show ip route** command when IP Routing is enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
Codes: > - best, C - connected, S - static
R - RIP
Policy Routing
VLAN 1
Route Map: BPR1
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.1
Next Hop Status: Active
ACL Name: ACLTCPTELNET
Next Hop: 2.2.2.2
Next Hop Status: Not Active (Unreachable)
ACL Name: ACL_AA
Next Hop: 3.3.3.3
Next Hop Status: Not Active (Not direct)
VLAN 100
Route Map: BPR_10
Status: Not Active (No IP interface on VLAN 100)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
```

```
VLAN 110
Route Map: BPR_20
Status: Not Active (VLAN 110 status is DOWN)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 200
Route Map: BPR_A0
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------- ------------
R> 10.7.10.0/24 120/5 10.119.254.244 00:02:22 vlan2
S> 10.175.0.0/16 1/1 10.119.254.240 00:02:22 vlan2
S> 10.180.0.0/16 1/1 10.119.254.240 00:02:42 vlan3
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

Example 3. In the following example, the logical AND operation is performed on the address 10.16.0.0 and the mask 255.255.0.0, resulting in 10.16.0.0. On each destination in the routing table the logical AND operation is also performed with the mask and the result is compared with 10.16.0.0. Any destinations that fall into that range are displayed in the output:

```
switchxxxxxx# show ip route 10.16.0.0 255.255.0.0 longer-prefix
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
R - RIP
Policy Routing
VLAN 1
Route Map: BPR1
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.1
Next Hop Status: Active
ACL Name: ACLTCPTELNET
Next Hop: 2.2.2.2
Next Hop Status: Not Active (Unreachable)
ACL Name: ACL_AA
Next Hop: 3.3.3.3
Next Hop Status: Not Active (Not direct)
VLAN 100
Route Map: BPR_10
Status: Not Active (No IP interface on VLAN 100)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 110
Route Map: BPR_20
Status: Not Active (VLAN 110 status is DOWN)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 200
Route Map: BPR_A0
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
IP Routing Table - 6 entries
```

```
Code IP Route Distance/ Next Hop Last Time Outgoing
Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------- ------------
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2
S> 10.16.2.64/26 1/1 100.1.14.244 00:02:22 vlan1
S> 10.16.2.128/26 1/1 110.9.2.2 00:02:22 vlan3
S> 10.16.208.0/24 1/1 120.120.5.44 00:02:22 vlan2
S> 10.16.223.0/24 1/1 20.1.2.24 00:02:22 vlan5
S> 10.16.236.0/24 1/1 30.19.54.240 00:02:23 vlan
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
C> 20.1.0.0/16 0/1 0.0.0.0 vlan5
C> 30.19.0.0/16 0/1 0.0.0.0 vlan2
C> 100.1.0.0/16 0/1 0.0.0.0 vlan1
C> 110.9.0.0/16 0/1 0.0.0.0 vlan3
C> 120.120.0.0/16 0/1 0.0.0.0 vlan2
```

Example 4. The following is sample output from the **show ip route** command when IP Routing is enabled and hardware forwarding is not active:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)
IP Forwarding: enabled (hardware forwarding is not active)
Directed Broadcast Forwarding: disabled
Codes: > - best, C - connected, S - static
Codes: > - best, C - connected, S - static
R - RIP
Policy Routin
VLAN 1
Route Map: BPR1
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.1
Next Hop Status: Active
ACL Name: ACLTCPTELNET
Next Hop: 2.2.2.2
Next Hop Status: Not Active (Unreachable)
ACL Name: ACL_AA
Next Hop: 3.3.3.3
Next Hop Status: Not Active (Not direct)
VLAN 100
Route Map: BPR_10
Status: Not Active (No IP interface on VLAN 100)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
VLAN 110
Route Map: BPR_20
Status: Not Active (VLAN 110 status is DOWN)
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Activ
VLAN 200
Route Map: BPR_A0
Status: Active
ACL Name: ACLTCPHTTP
Next Hop: 1.1.1.20
Next Hop Status: Active
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
Metric IP Address Updated Interface
------ ------------------ ----------- --------------- ------------- ------------
R> 10.7.10.0/24 120/5 10.119.254.244 00:02:22 vlan2
S> 10.175.0.0/16 1/1 10.119.254.240 00:02:22 vlan2
```

```
S> 10.180.0.0/16 1/1 10.119.254.240 00:02:42 vlan3
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

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

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Example

The following is sample output from the show **ip route summary** command:

```
switchxxxxxx# show ip route summary
IP Routing Table Summary - 90 entries
35 connected, 25 static, 12 RIP
Number of prefixes:
/16: 16, /18: 10, /22: 15, /24: 15, /28: 2, /30: 12
```

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

User Guidelines

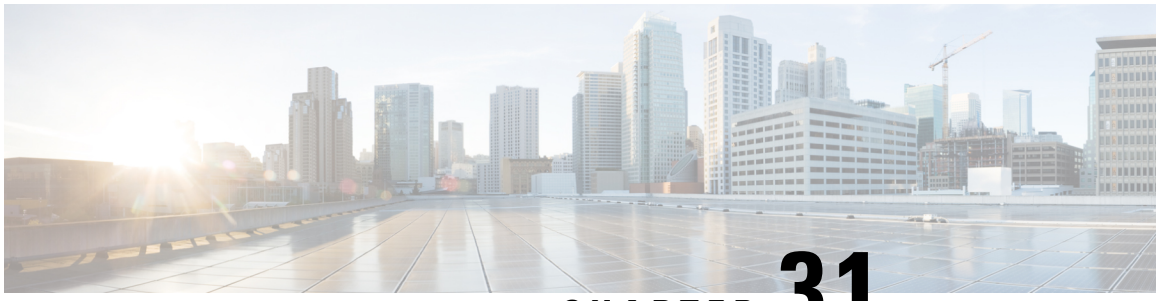
Examples

Example 1. The following is sample output from the **show key chain** command when the current time of date is defined:

```
switchxxxxxx# show key chain
Current Time of Date is Feb 8 2023
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 2021) - (23:59:59 Dec 5 2025)
send lifetime (06:00:00 Dec 5 2021) - (18:00:00 Dec 5 2026)[valid now]
```

Example 2. The following is sample output from the **show key chain** command when the current time of date is not defined:

```
switchxxxxxx# 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)
```



CHAPTER 31

IP System Management Commands

This chapter contains the following sections:

- ping, on page 475
- ssh, on page 477
- telnet, on page 478
- traceroute, on page 481

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*] [**source** *source-address*]

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

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.
- ***hostname***—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- **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).
- **source** *source-address*—Source address (Unicast IPv4 address or global Unicast IPv6 address).

Command Mode

Privileged 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.

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.

When the **source** keyword is configured and the source address is not an address of the switch, the command is halted with an error message and pings are not sent.

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 66.218.71.198: icmp_seq=0. time=11 ms
64 bytes from 66.218.71.198: icmp_seq=1. time=8 ms
64 bytes from 66.218.71.198: icmp_seq=2. time=8 ms
64 bytes from 66.218.71.198: 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 FF02::1: icmp_seq=1. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=0 ms
64 bytes from FF02::1: icmp_seq=1. time=1050 ms
64 bytes from FF02::1: icmp_seq=2. time=70 ms
64 bytes from FF02::1: icmp_seq=2. time=1050 ms
64 bytes from FF02::1: icmp_seq=3. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=70 ms
64 bytes from FF02::1: icmp_seq=4. time=0 ms
64 bytes from FF02::1: icmp_seq=3. time=1050 ms
64 bytes from FF02::1: icmp_seq=4. time=70 ms
64 bytes from FF02::1: icmp_sq=4. time=1050 ms
---- FF02::1 PING Statistics----
4 packets transmitted, 12 packets received
```

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in user EXEC or privileged EXEC mode.

Syntax

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

Parameters

- ***ip-address***—Specifies the destination host IP address (IPv4 or IPv6).
- ***hostname***—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- ***port***—Specifies the decimal TCP port number. The default port is the SSH port (22).
- ***keyword***—Specifies the one or more keywords listed in the Keywords table in the User Guidelines.

Keywords Table

Options	Description
/password *password*	Specifies the password to use when logging in on the remote networking device running the SSH server. If the keyword is not specified, the password configured by the **ip ssh-client password** command is used. If this keyword is specified the the **/user** keyword must be specified too.
/source-interface *interface-id*	Specifies the source interface which minimal IPv4/v6 address will be used as the source IPv4/v6 address. If the keyword is not specified, the source IPv4/IPv6 address configured by the **ip ssh-client source-interface** command is used.

Options	Description
/user *user-name*	Specifies the user name to use when logging in on the remote networking device running the SSH server. If the keyword is not specified, the user name configured by the **ip ssh-client username** command is used. If this keyword is specified the **/password** keyword must be specified too.

Default Configuration

The default port is the SSH port (22) on the host.

Command Mode

Privileged EXEC mode

User Guidelines

The **ssh** command enables the switch to make a secure, encrypted connection to another switch running an SSH server. This connection provides functionality that is similar to that of a Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Only one SSH terminal connection can be active at the same time.

Example 1. The following example sets a secure session between the local device and the edge device HQedge.

```
switchxxxxxx> ssh HQedge
```

Example 2. The following example sets a secure session between the local device and the edge device 1.1.1.1. The user name is HQhost and the password is a password configured by the **ip ssh-client password** command.

```
switchxxxxxx> ssh 1.1.1.1 /user HQhost
```

Example 3. The following example sets a secure session between the local device and the edge device HQedge. The user name is HQhost and the password is ar3245ddd.

```
switchxxxxxx> ssh HQedge /user HQhost /password ar3245ddd
```

Example 4. The following example sets a lookback interface as a source interface:

```
switchxxxxxx> ssh HQedge /source-interface loopback1
```

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***—Hostname to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- ***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

Privileged 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

Keyword	Description	Port Number
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
```

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*]

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

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 to ping (Length: 1-158 characters. Maximum label size for each part of the host name: 58.)
- **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)

Command Mode

Privileged 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 ipv6** 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
```

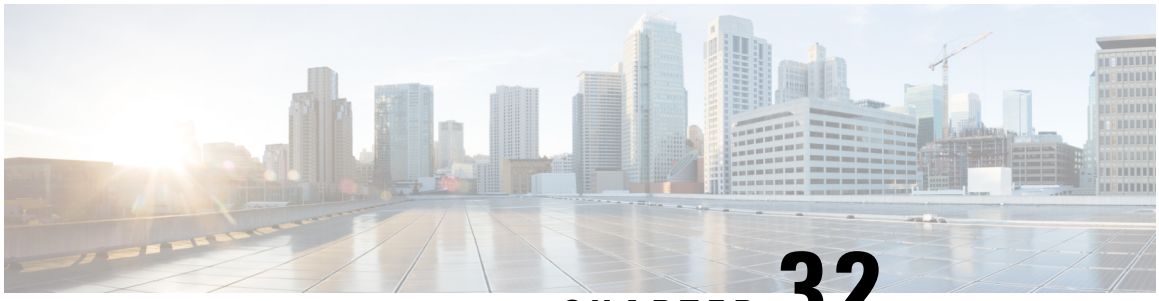
```
2 STAN.POS.calren2.NET (171.64.1.213) 0 msec 0 msec 0 msec
3 SUNV--STAN.POS.calren2.net (198.32.249.73) 1 msec 1 msec 1 msec
4 Abilene--QSV.POS.calren2.net (198.32.249.162)  1 msec 1 msec 1 msec
5 kscyng-snvang.abilene.ucaid.edu (198.32.8.103)  33 msec 35 msec 35 msec
6 iplsng-kscyng.abilene.ucaid.edu (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.



CHAPTER 32

IPv4 IPM Router Commands

This chapter contains the following sections:

- ip multicast-routing, on page 485
- ip multicast ttl-threshold, on page 486
- show ip mroute, on page 486
- show ip multicast, on page 488

ip multicast-routing

To enable IPv4 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 igmp-proxy

no ip multicast-routing

Parameters

- **igmp-proxy**—Enable Multicast routing using IGMP Proxy.

Default Configuration

Multicast routing is not enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **ip multicast-routing** command with parameter to specify the needed IP Multicast Routing Protocol.

To forward IPv4 Multicast packets on an interface, IPv4 Multicast forwarding must be enabled globally and an IPMv4 Routing protocol must be enabled on the interface.

Example

The following example enables IP Multicast routing using IGMP Proxy:

```
switchxxxxxx(config)# ip multicast-routing igmp-proxy
```

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 mode

User Guidelines

Multicast packets with a TTL value less than the threshold will not be forwarded on the interface. The default value of 0 means all Multicast packets are forwarded on the interface.

A value of 256 means that no Multicast packets are forwarded on 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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip multicast ttl-threshold 200
switchxxxxxx(config-if)# exit
```

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***—Destination Multicast IP address.
- ***source-address***—Source IP address.
- **summary**—Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.

Command Mode

User EXEC mode

Privileged EXEC mode

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]).

Examples

Description of Significant fields in the examples below

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.

Incoming interface: —Expected interface for a Multicast packet from the source. If the packet is not received on this interface, it is discarded.

Outgoing Interface List (OIF):—Interfaces through which packets will be forwarded.

Example 1. The following is sample output from the **show ip mroute** command with the summary keyword:

```
switchxxxxxx# show ip mroute summary
Timers: Uptime/Expires
IP Multicast Routing Table
(172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, OIF count:2
(172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, OIF count:
(172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, OIF count:2
(172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, OIF count:2
(172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, OIF count:2
(172.16.60.189/32, 224.2.127.254), 00:03:47/00:00:46, OIF count:2
```

Example 2. The following is sample output from the **show ip mroute** command:

```
switchxxxxxx# show ip mroute
Timers: Uptime/Expires
IP Multicast Routing Table
(*, 224.0.255.3), 5:29:15/00:03:01
Incoming interface: vlan2
Outgoing interface list:
vlan100, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), 05:29:15/00:02:59
Incoming interface: vlan2
Outgoing interface list:
vlan5, 05:29:15/00:02:57
```

show ip multicast

To display general information about IP Multicast configuration, 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 mode

Privileged EXEC mode

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 specified interface.

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:

```
switchxxxxxx# 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:

```
switchxxxxxx# 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 is an IGMP Proxy Upstream interface:

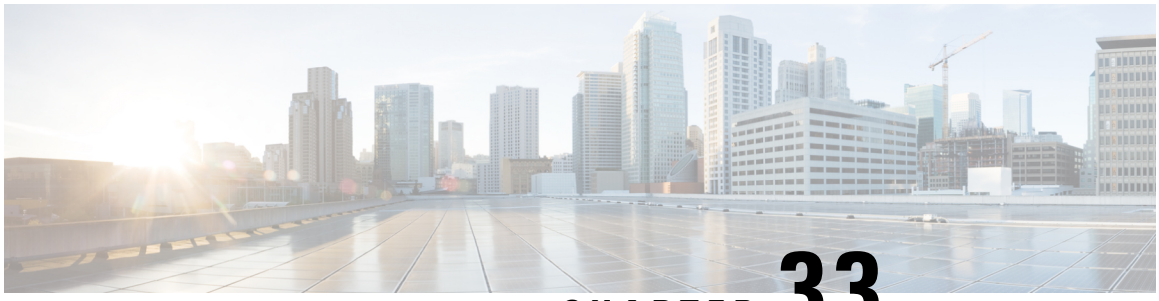
```
switchxxxxxx# show ip multicast interface vlan 200
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
TTL-threshold: 0
IGMP Protocol: IGMPv3
IGMP Proxy: Upstream
```

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:

```
switchxxxxxx# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGP Proxy
vlan 200
TTL-threshold: 0
IGMP Protocol: IGMPv3
IGMP Proxy: DownStream (Upstream: vlan 200)
```

Example 5. The following is sample output from the **show ip multicast** command about the given interface. IGMP Proxy is disabled on the interface:

```
switchxxxxxx# show ip multicast interface vlan 100
IP Unicast Forwarding: enabled
IP Multicast Protocol: IGMP Proxy
vlan 200
IP Status: enabled
hop-threshold: 100
IGMP Protocol: IGMPv3
IGMP Proxy: disabled
```



CHAPTER 33

IPv6 Commands

This chapter contains the following sections:

- clear ipv6 neighbors, on page 492
- distribute-list prefix-list (IPv6 OSPF), on page 492
- ipv6 address, on page 493
- ipv6 address anycast, on page 494
- ipv6 address autoconfig, on page 495
- ipv6 address eui-64, on page 496
- ipv6 address link-local, on page 497
- ipv6 default-gateway, on page 498
- ipv6 enable, on page 498
- ipv6 hop-limit, on page 499
- ipv6 icmp error-interval, on page 500
- ipv6 link-local default zone, on page 501
- ipv6 nd advertisement-interval, on page 501
- ipv6 nd dad attempts, on page 502
- ipv6 nd hop-limit, on page 503
- ipv6 nd managed-config-flag, on page 504
- ipv6 nd prefix, on page 505
- ipv6 nd ra interval, on page 507
- ipv6 nd ra lifetime, on page 508
- ipv6 nd ra suppress, on page 509
- ipv6 nd reachable-time, on page 510
- ipv6 nd router-preference, on page 511
- ipv6 neighbor, on page 512
- ipv6 policy route-map, on page 513
- ipv6 redirects, on page 514
- ipv6 route, on page 515
- ipv6 unicast-routing, on page 516
- ipv6 unreachables, on page 517
- show ipv6 interface, on page 517
- show ipv6 link-local default zone, on page 523
- show ipv6 nd prefix, on page 524
- show ipv6 neighbors, on page 525

- show ipv6 route, on page 526
- show ipv6 route summary, on page 528
- show ipv6 static, on page 528

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

Command Mode

Privileged EXEC mode

User Guidelines

Example

The following example deletes all entries, except static entries, in the neighbor discovery cache:

```
switchxxxxxx# clear ipv6 neighbors
```

distribute-list prefix-list (IPv6 OSPF)

Use the distribute-list prefix-list command in Router Configuration mode to apply a prefix list to the Open Shortest Path First (OSPF) for IPv6 routing updates that are received or sent on an interface.

To remove the prefix list, use the no form of this command.

Syntax

distribute-list prefix-list *list-name* {in [*interface-id]* | *out routing-process*}

no distribute-list prefix-list *list-name* {in [interface-id] | out routing-process}

Parameters

- *list-name*—Name of a prefix list, which defines which OSPF for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based on matching the network prefix to the prefixes in the list.
- *in*—Applies the prefix list to incoming routing updates on the specified interface.
- *interface-id*—Interface identifier
- *out*—Restricts which prefixes OSPF for IPv6 will identify to the other protocol.
- *routing-process*—Name of a specific routing process.

Default Configuration

Prefix lists are not applied to OSPF for IPv6 routing updates.

Command Mode

Router OSPF Configuration mode.

User Guidelines

If no interface is specified, the prefix list is applied to all interfaces.

Example

The following example applies the prefix list PL1 to routes received on VLAN 100, and applies the prefix list PL2 to advertised routes that came from process bgp 65:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# distribute-list prefix-list PL1 in vlan 100
switchxxxxxx(config-ospf)# exit
```

ipv6 address

Use the **ipv6 address** command in Interface Configuration mode to configure a global unicast 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 global unicast IPv6 address 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 mode

User Guidelines

The **ipv6 address** command cannot be applied to define an IPv6 address on an ISATAP interface.

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
switchxxxxxx(config-if)# exit
```

ipv6 address anycast

Use the **ipv6 address anycast** command in Interface Configuration mode to configure a global unicast 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*]

Parameters

- ***ipv6-address***—Specifies the global unicast IPv6 address 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 mode

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.

The **ipv6 address anycast** command cannot be applied to define an IPv6 address on an ISATAP interface.

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
switchxxxxxx(config-if)# exit
```

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 disable automatic configuration of IPv6 addresses and to remove the automatically configured address from the interface, use the **no** form of this command.

Syntax

ipv6 address autoconfig

no ipv6 address autoconfig

Default Configuration

Stateless Auto configuration is enabled.

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.

Additionally the **ipv6 address autoconfig** command enables on the interface the DHCPv6 Stateless client to receive DHCP stateless information and this information is received from a DHCPv6 server regardless whether IPv6 Forwarding is enabled or not.

Example

The following example assigns the IPv6 address automatically:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 address autoconfig
switchxxxxxx(config-if)# exit
```

ipv6 address eui-64

Use the **ipv6 address eui-64** command in Interface Configuration mode to configure a global unicast 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-prefix***—Specifies the global unicast IPv6 address 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 mode

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.

The IPv6 address is built from *ipv6-prefix* and the EUI-64 Interface ID by the following way:

- The first *prefix-length* bits are taken from *ipv6-prefix*.
- If *prefix-length* < 64 then

  The following (64-*prefix-length*) bits are filled by 0s.

  - The last 64 bits are taken from the EUI-64 Interface ID.

- If *prefix-length* equals to 64 then the following 64 bits are taken from the EUI-64 Interface ID.

- If *prefix-length* > 64 then the following (128-*prefix-length*) bits are taken from the last (64-(*prefix-length* -64)) bits of the EUI-64 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.

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
switchxxxxxx(config-if)# exit
```

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 mode

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.

The **ipv6 address link-local** command cannot be applied to define an IPv6 address on an ISATAP interface.

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
switchxxxxxx(config-if)# exit
```

ipv6 default-gateway

Use the **ipv6 default-gateway** Global Configuration mode command to define an IPv6 default gateway. To remove the IPv6 default gateway, use the **no** form of this command.

Syntax

ipv6 default-gateway {*ipv6-address* [*outgoing-interface-id*]} | *interface-id*

no ipv6 default-gateway *[{ipv6-address* [*outgoing-interface-id*]} | *interface-id*]

Parameters

- ***ipv6-address***—Specifies the IPv6 address of an IPv6 router that can be used to reach a network.
- ***outgoing-interface-id***—Outgoing Interface identifier.
- ***interface-id***—Specifies the Interface Identifier of the outgoing interface that can be used to reach a network. This argument can be applied only to point-to-point interfaces (manual IPv6 over IPv4 tunnels).

Default Configuration

No default gateway is defined.

Command Mode

Global Configuration mode

Example 1. The following example defines a default gateway with a global IPv6 address:

```
switchxxxxxx(config)# ipv6 default-gateway 5::5
```

Example 2. The following example defines a default gateway with a link-local IPv6 address:

```
switchxxxxxx(config)# ipv6 default-gateway  FE80::260:3EFF:FE11:6770%vlan1
```

Example 3. The following example defines a default gateway on manual tunnel 1:

```
switchxxxxxx(config)# ipv6 default-gateway tunnel1
```

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

Default Configuration

IPv6 interface is disabled.

Command Mode

Interface Configuration mode

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.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 enable
switchxxxxxx(config-if)# exit
```

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 mode

Example

The following example configures a maximum number of 15 hops for all IPv6 packets that are originated from the router:

```
switchxxxxxx(config)# ipv6 hop-limit 15
```

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:

```
switchxxxxxx(config)# ipv6 icmp error-interval 50 20
```

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:

```
switchxxxxxx(config)# ipv6 link-local default zone vlan1
```

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

i**pv6 nd advertisement-interval**

no ipv6 nd advertisement-interval

Default Configuration

Advertisement interval option is not sent.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd advertisement-interval
switchxxxxxx(config-if)# exit
```

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 mode

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.

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. Since DAD is not supported on NBMA interfaces the command is allowed but does not impact on an IPv6 tunnel interface of the ISATAP type it does not impact. 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.

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd dad attempts 5
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 nd dad attempts 0
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 nd hop-limit 15
switchxxxxxx(config-if)# exit
```

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

Default Configuration

The “managed address configuration flag” flag is not set in IPv6 router advertisements.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd managed-config-flag
switchxxxxxx(config-if)# exit
```

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 mode

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*/*prefix-length* command to remove the prefix from the Prefix table.

Use the **no ipv6 nd prefix** command without the *ipv6-prefix*/*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 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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900
switchxxxxxx(config-if)# exit
```

Example 2. The following example advertises the prefix with the L-bit clear:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 address 2001::1/64
switchxxxxxx(config-if)# ipv6 nd prefix 2001::/64 3600 3600 no-onlink
switchxxxxxx(config-if)# exit
```

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 mode

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 1. The following example configures an IPv6 router advertisement interval of 201 seconds for VLAN 1:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra interval 201
switchxxxxxx(config-if)# exit
```

Example 2. The following examples shows a maximum RA interval of 200 seconds and a minimum RA interval of 50 seconds:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra interval 200 50
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra lifetime 1801
switchxxxxxx(config-if)# exit
```

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

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 mode

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).

NBMA interface - IPv6 router advertisements are suppressed.

Use the **no ipv6 nd ra suppress** command to enable the sending of IPv6 router advertisement transmissions on a NBMA interface (for example, ISATAP tunnel).

Example 1. The following example suppresses IPv6 router advertisements on vlan 1:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd ra suppress
switchxxxxxx(config-if)# exit
```

Example 2. The following example enables the sending of IPv6 router advertisements on tunnel 1:

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# no ipv6 nd ra suppress
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd reachable-time 1700000
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 nd router-preference high
switchxxxxxx(config-if)# exit
```

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 mode

User Guidelines

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.

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 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:

```
switchxxxxxx(config)# 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:

```
switchxxxxxx(config)# 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:

```
switchxxxxxx(config)# no ipv6 neighbor vlan1
```

Example 4. The following example deletes all static entries in the IPv6 neighbor discovery cache on all interfaces:

```
switchxxxxxx(config)# no ipv6 neighbor
```

ipv6 policy route-map

To enable policy routing on an interface and identify a route map, use the **ipv6 policy route-map** command in Interface Configuration mode. To disable policy routing, use the **no** form of this command.

Syntax

ipv6 policy route-map *map-tag*

no ipv6 policy route-map

Parameters

- ***map-tag***—Name of the route map to use for policy routing.

Default Configuration

No policy routing occurs on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the **ipv6 policy route-map** command to enable IPv6 policy routing.

Use the **ipv6 policy route-map** command to enable policy routing on an interface. The actual policy routing will take a place if an IPv6 is enabled on the interface.

The IPv6 packets matched to the route-map conditions specified by the route map with the *map-tag* name will take a route depended on the action of the matched ACL:

- **permit**—The route specified by the set command Policy routing.

- **deny**—The route specified by the IPv6 Forwarding table (regular routing).
- Name of the route map to use for policy routing.

The not matched IPv6 packets will be forwarded using the obvious shortest path.

IPv6 policy routing on a Layer 2 interface is performed only when IPv6 interface is defined, its status is UP, and the next hop is reachable. If the IPv6 policy routing is not applied then the matched IPv6 packets will be forwarded using the obvious shortest path.

Note. Of course, like in the case of regular IPv6 Routing Policy Based IPv6 Router routes only MAC "tome" IPv6 frames.

IPv6 policy routing cannot be configured on an interface together with the following features:

- IPv6 First Hop Security
- VLAN ACL
- VLAN Rate Limit

Example

The following example shows how to configure policy routing:

```
switchxxxxxx(config)# ipv6 access-list pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 3002:08FA/32 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# ipv6 access-list pr-acl2
switchxxxxxx(config-ip-al)# permit tcp any any 3002:0800/32 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr 10
switchxxxxxx(config-route-map)# match ipv6 address access-list pr-acl1
switchxxxxxx(config-route-map)# set ipv6 next-hop 3012:12af::1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# route-map pbr 20
switchxxxxxx(config-route-map)# match ipv6 address access-list pr-acl2
switchxxxxxx(config-route-map)# set ipv6 next-hop 3012:1223::1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 policy route-map pbr
switchxxxxxx(config-if)# exit
```

ipv6 redirects

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 redirects

no ipv6 redirects

Default Configuration

The sending of ICMP IPv6 redirect messages is enabled.

Command Mode

Interface Configuration mode

Example

The following example disables the sending of ICMP IPv6 redirect messages on VLAN 100 and re-enables the messages on VLAN 2:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 redirects
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# ipv6 redirects
switchxxxxxx(config-if)# exit
```

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* [*outgoing-interface-id*]} | *interface-id*} [*metric*]

no ipv6 route *ipv6-prefix*/*prefix-length* [{*next-ipv6-address* [*outgoing-interface-id*]} | *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.
- ***outgoing-interface-id***—Outgoing Interface identifier.
- ***interface-id***—Outgoing Interface identifier. This argument can be applied only to point-to-point interfaces (manual IPv6 over IPv4 tunnels).
- ***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 mode

User Guidelines

Use the **ipv6 route** *ipv6-prefix/prefix-length interface-id* [*metric*] command to define a static route, if the outgoing interface is a manual tunnel.

If the *next-ipv6-address* argument is a global IPv6 address that belongs to an on-link prefix you can omit the *outgoing-interface-id* argument and in this case the L2 interface on which this on-link prefix is defined will be used as the outgoing interface. If the *outgoing-interface-id* argument is configured it overrides this switch decision.

If the *next-ipv6-address* argument is a global IPv6 address that does not belong to any on-link prefix you must configure the *outgoing-interface-id* argument.

If the *next-ipv6-address* argument is a link-local IPv6 address and the *outgoing-interface-id* argument is omitted the zone of the *next-ipv6-address* argument will be used as the outgoing interface. If the *outgoing-interface-id* argument is configured it overrides this zone.

Example 1. The following example defines a static route with a global next hop:

```
switchxxxxxx(config)# ipv6 route 2001::/64 5::5 10
```

Example 2. The following example defines a static route with a link-local next hop:

```
switchxxxxxx(config)# ipv6 route 2001:DB8:2222::/48 FE80::260:3EFF:FE11:6770%vlan1 12
```

Example 3. The following example defines a static route on manual tunnel 1:

```
switchxxxxxx(config)# ipv6 route 2001:DB8:2222::/48 tunnel1
```

Example 4. The following example defines a static route on with the outgoing interface:

```
switchxxxxxx(config)# ipv6 route 2001::/64 5::5 vlan10 10
```

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

Default Configuration

IPv6 Unicast routing is disabled.

Command Mode

Global Configuration mode

Example

The following example enables the forwarding of IPv6 Unicast datagrams:

```
switchxxxxxx(config)# ipv6 unicast-routing
```

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

Default Configuration

The sending of ICMP IPv6 unreachable messages is enabled.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# no ipv6 unreachables
switchxxxxxx(config-if)# exit
```

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 mode

Privileged EXEC mode

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.

The keyword is supported only if IPv6 unicast routing is enabled.

Example 1. The show ipv6 interface command displays information about the specified interface:

```
switchxxxxxx# 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.
Stateless autoconfiguration is not available (IPv6 Forwarding 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.
- **MTU is 1500 bytes**—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:

```
switchxxxxxx# 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.
Stateless autoconfiguration is disabled.
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 mode**—Specifies the tunnel mode: **manual**
- **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 ISATAP tunnel:

```
switchxxxxxx# 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
Stateless autoconfiguration is disabled.
MLD Version is 2
Tunnel mode is ISATAP
Tunnel Local IPv4 address : 10.10.10.1(VLAN 1)
ISATAP Router DNS name is isatap
Field Descriptions:
```

- **ND DAD**—The state of duplicate address detection on the interface (enabled or disabled). **Note.** The state of duplicate address detection on an IPv6 tunnel interface of ISATAP type always is displayed as disabled regardless of a value of the **number of DAD attempts** parameter because DAD is not supported on NBMA interfaces. 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 mode**—Specifies the tunnel mode: **isatap**
- **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

- **ISATAP Router DNS name is**—The DNS name of the ISATAP Router

Example 4. The following command with the **brief** keyword displays information about all interfaces that IPv6 is defined on:

```
switchxxxxxx# show ipv6 interface brief
Interface  Interface  IPv6     Link Local        MLD        Number of
             State     State   IPv6 Address     Version  Global Addresses
---------  --------- -------  ----------------- -------   ----------------
vlan 1     up/up     enabled  FE80::0DB8:12AB:FA01        1                            1
vlan 2     up/up     stalled  FE80::0DB8:12AB:FA01        1                            1
vlan 3     up/down   enabled  FE80::0DB8:12AB:FA01        1                             3
vlan 4     down/down enabled  FE80::0DB8:12AB:FA01         2                            2
vlan 5     up/up     enabled  FE80::0DB8:12AB:FA01        1                             1
vlan 100   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:

```
switchxxxxxx# configure terminal
switchxxxxxx(config)# interface vlan1
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:1::1/64
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:2::1/64
switchxxxxxx(config-if)# ipv6 address 2001:0DB8:3::1/64
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:1::/64 no-advertise
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:3::/64 2912000 564900 off-link
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:4::/64
switchxxxxxx(config-if)# ipv6 nd prefix 2001:0DB8:5::/64 2912000 564900 off-link
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# exit
switchxxxxxx# 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
```

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

User EXEC mode

Privileged EXEC mode

Example 1. The following example displays the default zone when it is defined:

```
switchxxxxxx# 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:

```
switchxxxxxx# show ipv6 link-local default zone
Link Local Default Zone is not defined
```

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

User EXEC mode

Privileged EXEC mode

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 IPv6 prefixes:

```
switchxxxxxx# 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
```

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 mode

Privileged EXEC mode

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 1. The following is sample output from the show ipv6 neighbors command when entered with an interface-id:

```
switchxxxxxx# 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:

```
switchxxxxxx# 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.

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 mode

Privileged EXEC mode

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 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:

```
switchxxxxxx# show ipv6 route
Codes: > - Best
       S - Static, C - Connected(from ipv6 address), I - ICMP Redirect, ND - Router
Advertisment
[d/m]: d - route’s distance, m - route’s metric
IPv6 Forwarding is disabled
IPv6 Routing Table - 4 entries
S> ::/0 [1/1]
   via:: fe80::77  VLAN 1
ND> ::/0   [3/2]
   via:: fe80::200:cff:fe4a:dfa8 VLAN 1 Lifetime 1784 sec
C> 3002:1:1:1:1/64   [0/0]
   via:: VLAN 1
ND> 3004:1:1:1:1/64   [0/0]
   via:: VLAN 100 Lifetime 1784 sec
```

Example 2. The following is sample output from the **show ipv6 route** command when IPv6 Routing is enabled and the command is entered without an IPv6 address or prefix specified:

```
switchxxxxxx# show ipv6 route
Codes: > - Best
    S - Static, C - Connected(from ipv6 address),
    L - Local(on-link prefixes defined by the ipv6 nd prefix command with on-link keyword,
[d/m]: d - route’s distance, m - route’s metric
IPv6 Forwarding is enabled (hardware forwarding is not active)
IPv6 Policy Routing
VLAN 1
   Route Map:   BPR1
   Status:   Active
      ACL Name: ACLTCPHTTP
         Next Hop: fe80::77
         Next Hop Status: Active
      ACL Name: ACLTCPTELNET
          Next Hop: 4001::27
          Next Hop Status: Not Active (Unreachable)
      ACL Name: ACL_AA
         Next Hop: 301a:23:24
         Next Hop Status: Not Active (Not direct)
VLAN 100
   Route Map:   BPR_10
   Status:   Not Active (No IP interface on VLAN 100)
      ACL Name: ACLTCPHTTP
        Next Hop: 4214::10
        Next Hop Status: Active
VLAN 110
   Route Map:   BPR_20
   Status:   Not Active (VLAN 110 status is DOWN)
      ACL Name: ACLTCPHTTP
        Next Hop: 3004:1241::73
        Next Hop Status: Active
```

```
VLAN 200
   Route Map:   BPR_A0
   Status:   Active
      ACL Name: ACLTCPHTTP
         Next Hop: 3004:1241::73
         Next Hop Status: Active
IPv6 Routing Table - 3 entries
S>   3000::/64 [1/1]
       via:: FE80::A8BB:CCFF:FE02:8B00   VLAN 100
C>   4001::/64 [0/0]
       via::   VLAN 100
L>   4002::/64 [0/0]
       via::   VLAN 100 Lifetime 9000 sec
```

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

Command Mode

User EXEC mode

Privileged EXEC mode

Example

The following is sample output from the show ipv6 route summary command:

```
switchxxxxxx# 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
```

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 mode

Privileged EXEC mode

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 1. The following is sample output from the **show ipv6 static** command without specified options:

```
switchxxxxxx# show ipv6 static
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 3000::/16, via outgoing interface tunnel1, metric 1
  5000::/16, via outgoing interface tunnel2, metric 1
* 5555::/16, via outgoing interface VLAN100 nexthop 4000::1 metric 1
  5555::/16, via outgoing interface VLAN10 nexthop 9999::1 vlan100 metric 1
* 5555::/16, via outgoing interface VLAN100 nexthop 4001:AF00::1,  metric 1
* 6000::/16, via outgoing interface VLAN1 nexthop 2007::1 metric 1
```

Example 2. The following is sample output from the **show ipv6 static** command when entered with the IPv6 prefix 2001:200::/35:

```
switchxxxxxx# show ipv6 static 2001:200::/35
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 2001:200::/35, via outgoing interface VLAN100 nexthop 4000::1, metric 1
   2001:200::/35, via outgoing interface VLAN10 nexthop 9999::1, metric 1
```

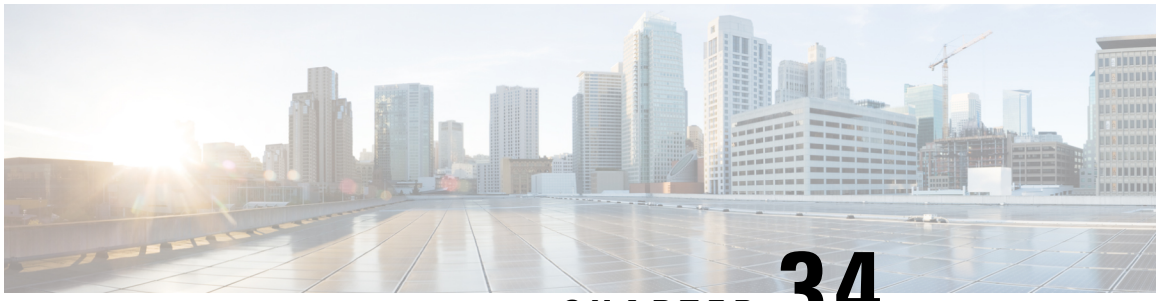
Example 3. The following is sample output from the **show ipv6 static** command when entered with the interface VLAN 1:

```
switchxxxxxx# show ipv6 static interface vlan 1
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
```

```
IPv6 Static routes distance is 1
* 5000::/16, via outgoing interface VLAN1 nexthop 4000::1, metric 1
```

Example 4. The following is sample output from the **show ipv6 static** command with the **detail** keyword:

```
switchxxxxxx# show ipv6 static detail
IPv6 Static routes   Code: * - installed in Forwarding Information Base (FIB)
IPv6 Static routes distance is 1
* 3000::/16, via outgoing interface tunnel1, metric 1
  5000::/16, via outgoing interface tunnel2, metric 1
  5000::/16, via outgoing interface VLAN2 nexthop 2003::1, metric 1
         Interface is down
* 5555::/16, via outgoing interface VLAN100 nexthop 4000::1, metric 1
  5555::/16, via outgoing interface VLAN10 nexthop 9999::1, metric 1
         Route does not fully resolve
* 5555::/16, via outgoing interface VLAN12 nexthop 4001:AF00::1, metric 1
* 6000::/16, via outgoing interface VLAN102 nexthop 2007::1, metric 1
```



CHAPTER 34

IPv6 First Hop Security

This chapter contains the following sections:

- address-config, on page 533
- address-prefix-validation, on page 534
- clear ipv6 first hop security counters, on page 534
- clear ipv6 first hop security error counters, on page 535
- clear ipv6 neighbor binding prefix table, on page 535
- clear ipv6 neighbor binding table, on page 536
- device-role (IPv6 DHCP Guard), on page 537
- device-role (Neighbor Binding), on page 538
- device-role (ND Inspection Policy), on page 539
- device-role (RA Guard Policy), on page 540
- drop-unsecure, on page 541
- hop-limit, on page 542
- ipv6 dhcp guard, on page 543
- ipv6 dhcp guard attach-policy (port mode), on page 544
- ipv6 dhcp guard attach-policy (VLAN mode), on page 545
- ipv6 dhcp guard policy, on page 546
- ipv6 dhcp guard preference, on page 547
- ipv6 first hop security, on page 548
- ipv6 first hop security attach-policy (port mode), on page 549
- ipv6 first hop security attach-policy (VLAN mode), on page 550
- ipv6 first hop security logging packet drop, on page 551
- ipv6 first hop security policy, on page 552
- ipv6 nd inspection, on page 553
- ipv6 nd inspection attach-policy (port mode), on page 553
- ipv6 nd inspection attach-policy (VLAN mode), on page 555
- ipv6 nd inspection drop-unsecure, on page 556
- ipv6 nd inspection policy, on page 556
- ipv6 nd inspection sec-level minimum, on page 558
- ipv6 nd inspection validate source-mac, on page 558
- ipv6 nd raguard, on page 559
- ipv6 nd raguard attach-policy (port mode), on page 560
- ipv6 nd raguard attach-policy (VLAN mode), on page 561

- ipv6 nd raguard hop-limit, on page 562
- ipv6 nd raguard managed-config-flag, on page 563
- ipv6 nd raguard other-config-flag, on page 564
- ipv6 nd raguard policy, on page 564
- ipv6 nd raguard router-preference, on page 566
- ipv6 neighbor binding, on page 567
- ipv6 neighbor binding address-config, on page 567
- ipv6 neighbor binding address-prefix, on page 569
- ipv6 neighbor binding address-prefix-validation, on page 570
- ipv6 neighbor binding attach-policy (port mode), on page 571
- ipv6 neighbor binding attach-policy (VLAN mode), on page 572
- ipv6 neighbor binding lifetime, on page 573
- ipv6 neighbor binding max-entries, on page 573
- ipv6 neighbor binding policy, on page 574
- ipv6 neighbor binding static, on page 576
- ipv6 source guard, on page 576
- ipv6 source guard attach-policy (port mode), on page 577
- ipv6 source guard policy, on page 578
- logging binding, on page 579
- logging packet drop, on page 580
- managed-config-flag, on page 581
- match ra address, on page 581
- match ra prefixes, on page 582
- match reply, on page 583
- match server address, on page 584
- max-entries, on page 585
- other-config-flag, on page 587
- preference, on page 587
- router-preference, on page 588
- sec-level minimum, on page 589
- show ipv6 dhcp guard, on page 590
- show ipv6 dhcp guard policy, on page 590
- show ipv6 first hop security, on page 592
- show ipv6 first hop security active policies, on page 592
- show ipv6 first hop security attached policies, on page 593
- show ipv6 first hop security counters, on page 594
- show ipv6 first hop security error counters, on page 595
- show ipv6 first hop security policy, on page 596
- show ipv6 nd inspection, on page 597
- show ipv6 nd inspection policy, on page 597
- show ipv6 nd raguard, on page 598
- show ipv6 nd raguard policy, on page 599
- show ipv6 neighbor binding, on page 600
- show ipv6 neighbor binding policy, on page 600
- show ipv6 neighbor binding prefix table, on page 602
- show ipv6 neighbor binding table, on page 602

- show ipv6 source guard, on page 604
- show ipv6 source guard policy, on page 604
- trusted-port (IPv6 Source Guard), on page 605
- validate source-mac, on page 606

address-config

To specify allowed configuration methods of global IPv6 addresses within an IPv6 Neighbor Binding policy, use the address-config command in Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

address-config [stateless | any] [dhcp]

no address-config

Parameters

- **stateless**—Only auto configuration for global IPv6 bound from NDP messages is allowed.
- **any**—All configuration methods for global IPv6 bound from NDP messages (stateless and manual) are allowed. If no keyword is defined the **any** keyword is applied.
- **dhcp**—Bound from DHCPv6 is allowed.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

If no keyword is defined the **address-config any** command is applied.

Example

The following example shows how to change the global configuration to allow only DHCP address configuration method:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-config dhcp
switchxxxxxx(config-nbr-binding)# exit
```

address-prefix-validation

To define the bound address prefix validation within an IPv6 Neighbor Binding policy, use the **address-prefix-validation** command in Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

address-prefix-validation [enable | disable]

no address-prefix-validation

Parameters

- **enable**—Enables bound address prefix validation. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables bound address prefix validation.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configured value.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

When a policy containing this command is attached to a VLAN, it overrides the global configuration and is applied to all ports of the VLAN. When this command is used in a policy attached to a port, it overrides the global and the VLAN configurations.

Example

The following example shows how to define policy1 that changes the global bound address verification in Neighbor Binding:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# address-prefix-validation enable
switchxxxxxx(config-nbr-binding)# exit
```

clear ipv6 first hop security counters

To clear IPv6 First Hop Security port counters, use the **clear ipv6 first hop security counters** command in privileged EXEC mode.

Syntax

clear ipv6 first hop security counters [interface *interface-id*]

Parameters

- **interface** *interface-id*—Clear IPv6 First Hop Security counters for the specified Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

This command clears port counters about packets handled by IPv6 First Hop Security.

Use the **interface** keyword to clear all counters for the specific port.

Use the command without keyword to clear all counters.

Example

The following example clears IPv6 First Hop Security counters on port gi1/0/1

```
switchxxxxxx# clear ipv6 first hop security counters interface gi1/0/1
```

clear ipv6 first hop security error counters

To clear IPv6 First Hop Security global error counters, use the **clear ipv6 first hop security error counters** command in privileged EXEC mode.

Syntax

clear ipv6 first hop security error counters

Command Mode

Privileged EXEC mode

User Guidelines

This command clears global error counters.

Example

The following example clears IPv6 First Hop Security error counters:

```
switchxxxxxx# clear ipv6 first hop security error counters
```

clear ipv6 neighbor binding prefix table

To remove dynamic entries from the Neighbor Prefix table, use the **clear ipv6 neighbor binding prefix table** command in Privilege EXEC configuration mode.

Syntax

clear ipv6 neighbor binding prefix table [**vlan** *vlan-id*] [*prefix-address*/*prefix-length*]

Parameters

- ***vlan-id***—Clear the dynamic prefixes that match the specified VLAN.
- ***prefix-address*/ *prefix-length***—Clear the specific dynamic prefix.

Command Mode

Privileged EXEC mode

User Guidelines

This command deletes the dynamic entries of the Neighbor Prefix table.

Use the **clear ipv6 neighbor binding prefix table vlan** *vlan-id prefix-address*/*prefix-length* command to delete one specific entry.

Use the **clear ipv6 neighbor binding prefix table vlan** *vlan-id* command to delete the dynamic entries that match the specified VLAN.

Use the **clear ipv6 neighbor binding prefix table** command to delete all dynamic entries.

Example 1. The following example clears all dynamic entries:

```
switchxxxxxx# clear ipv6 neighbor binding prefix table
```

Example 2. The following example clears all dynamic prefixes that match VLAN 100:

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100
```

Example 3. The following example clears one specific prefix:

```
switchxxxxxx# clear ipv6 neighbor binding prefix table vlan 100 2002:11aa:0000:0001::/64
```

clear ipv6 neighbor binding table

To remove dynamic entries from the Neighbor Binding table, use the **clear ipv6 neighbor binding table** command in Privilege EXEC configuration mode.

Syntax

clear ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*] [**ndp** | **dhcp**]

Parameters

- **vlan** *vlan-id*—Clear the dynamic entries that match the specified VLAN.
- **interface** *interface-id*—Clear the dynamic entries that match the specified port (Ethernet port or port channel).
- **ipv6** *ipv6-address*—Clear the dynamic entries that match the specified IPv6 address.

- **mac** *mac-address*—Clear the dynamic entries that match the specified MAC address.
- **ndp**—Clear the dynamic entries that are bound from NDP messages.
- **dhcp**—Clear the dynamic entries that are bound from DHCPv6 messages.

Command Mode

Privileged EXEC mode

User Guidelines

This command deletes the dynamic entries of the Neighbor Binding table. The dynamic entries to be deleted can be specified by the *vlan-id* argument, the *interface-id* argument, IPv6 address, MAC address, or by type of message from which they were bound.

If the **ndp** keyword and the **dhcp** keyword is not defined, the entries are removed regardless their origin. If no keywords or arguments are entered, all dynamic entries are deleted. All keyword and argument combinations are allowed.

Example

The following example clears all dynamic entries that exist on VLAN 100 & port gi1/0/1:

```
switchxxxxxx# clear ipv6 neighbor binding table vlan 100 interface gi1/0/1
```

device-role (IPv6 DHCP Guard)

To specify the role of the device attached to the port within an IPv6 DHCP Guard policy, use the **device-role** command in IPv6 DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

device-role {client | server}

no device-role

Parameters

- **client**—Sets the role of the device to DHCPv6 client.
- **server**—Sets the role of the device to DHCPv6 server.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: client.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

IPv6 DHCP Guard discards the following DHCPv6 messages sent by DHCPv6 servers/relays and received on ports configured as client:

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

Example

The following example defines an IPv6 DHCP Guard policy named policy 1 and configures the port role as the server:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

device-role (Neighbor Binding)

To specify the role of the device attached to the port within an IPv6 Neighbor Binding policy, use the **device-role** command within IPv6 Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

device-role {perimeter | internal}

no device-role

Parameters

- **perimeter**—Specifies that the port is connected to devices not supporting IPv6 First Hop Security.
- **internal**—Specifies that the port is connected to devices supporting IPv6 First Hop Security.

Default Configuration

Policy attached to port or port channel: Value configured in the policy attached to the VLAN.

Policy attached to VLAN: Perimeter.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

NB Integrity supports the perimetrical model (see RFC 6620).

This model specifies two types of ports:

- **Perimeter Port**—Specifies ports connected to devices not supporting NB Integrity. NB Integrity establishes binding for neighbors connected to these ports. Source Guard does not function on these ports.
- **Internal Port**—The second type specifies ports connected to devices supporting IPv6 First Hop Security. NB Integrity does not establish binding for neighbors connected to these ports, but it does propagate the bindings established on perimeter ports.

A dynamic IPv6 address bound to a port is deleted when its role is changed from perimetrical to internal. A static IPv6 address is kept.

Example

The following example defines a Neighbor Binding policy named policy 1 and configures the port role as an internal port:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
```

device-role (ND Inspection Policy)

To specify the role of the device attached to the port within an IPv6 ND Inspection policy, use the **device-role** command in ND Inspection Policy Configuration mode. To disable this function, use the **no** form of this command.

Syntax

device-role {host | router}

no device-role

Parameters

- **host**—Sets the role of the device to host.
- **router**—Sets the role of the device to router.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: host.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

ND Inspection performs egress filtering of NDP messages depending on a port role.The following table specifies the filtering rules.

Message	Host	Router
RA	Permit	Permit
RS	Deny	Permit
CPA	Permit	Permit
CPS	Deny	Permit
ICMP Redirect	Permit	Permit

Example

The following example defines an ND Inspection policy named policy 1 and configures the port role as router:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

device-role (RA Guard Policy)

To specify the role of the device attached to the port within an IPv6 RA Guard policy, use the **device-role** command in RA Guard Policy Configuration mode. To returned to the default, use the **no** form of this command.

Syntax

device-role {host | router}

no device-role

Parameters

- **host**—Sets the role of the device to host.
- **router**—Sets the role of the device to router.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: host.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

RA Guard discards input RA, CPA, and ICMPv6 Redirect messages received on ports configured as host.

Example

The following example defines an RA Guard policy named policy 1 and configures the port role as **router**:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

drop-unsecure

To enable dropping messages with no or invalid options or an invalid signature within an IPv6 ND Inspection policy, use the drop-unsecure command in ND Inspection Policy Configuration mode. To return to the default, use the no form of this command.

Syntax

drop-unsecure [enable | disable]

no drop-unsecure

Parameters

- **enable**—Enables dropping messages with no or invalid options or an invalid signature. If no keyword is configured this keyword is applied by default.
- **disable**—Disables dropping messages with no or invalid options or an invalid signature.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example defines an ND Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and enables the switch to drop messages with no or invalid options or an invalid signature:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# exit
```

hop-limit

To enable the verification of the advertised Cur Hop Limit value in RA messages within an IPv6 RA Guard policy, use the **hop-limit** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

hop-limit {[maximum {*value* | disable}] [minimum {*value* | disable}]}

no hop-limit [maximum] [minimum]

Parameters

- **maximum** *value*—Verifies that the hop-count limit is less than or equal to the **value** argument. Range 1-255. The value of the high boundary must be equal or greater than the value of the low boundary.
- **maximum disable**—Disables verification of the high boundary of the hop-count limit.
- **minimum** *value*—Verifies that the hop-count limit is greater than or equal to the **value** argument. Range 1-255.
- **minimum disable**—Disables verification of the lower boundary of the hop-count limit.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Use the **disable** keyword to disable verification regardless of the global or VLAN configuration.

Example 1—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and defines a minimum Cur Hop Limit value of 5:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit minimum 5
switchxxxxxx(config-ra-guard)# exit
```

Example 2—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and disables validation of the Cur Hop Limit high boundary:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# hop-limit maximum disable
switchxxxxxx(config-ra-guard)# exit
```

ipv6 dhcp guard

To enable the DHCPv6 guard feature on a VLAN, use the **ipv6 dhcp guard** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard

no ipv6 dhcp guard

Default Configuration

DHCPv6 Guard on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

DHCPv6 Guard blocks messages sent by DHCPv6 servers/relays to clients received on ports that are not configured as a DHCPv6 server. Client messages or messages sent by relay agents from clients to servers are not blocked.

DHCPv6 Guard validates received DHCPv6 messages based on a DHCPv6 Guard policy attached to the source port.

Example 1—The following example enables DHCPv6 Guard on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables DHCPv6 Guard on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 dhcp guard
switchxxxxxx(config-if-range)# exit
```

ipv6 dhcp guard attach-policy (port mode)

To attach a DHCPv6 Guard policy to a specific port, use the **ipv6 dhcp guard attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 dhcp guard attach-policy [*policy-name*]

Parameters

- ***policy-name***—The DHCPv6 Guard policy name (up to 32 characters).
- **vlan** *v*lan-list—Specifies that the DHCPv6 Guard policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which DHCPv6 Guard is enabled.

Default Configuration

The DHCPv6 Guard default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach a DHCPv6 Guard policy to a port.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use **no ipv6 dhcp guard attach-policy** to detach all user-defined DHCP Guard policies attached to the port.

Use **no ipv6 dhcp guard attach-policy** *policy-name* to detach the specific policy from the port.

Example 1—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/0/1 port and the default policy port_default is detached:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the DHCPv6 Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the DHCPv6 Guard policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example DHCPv6 Guard detaches policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard attach-policy (VLAN mode)

To attach a DHCPv6 Guard policy to a specified VLAN, use the **ipv6 dhcp guard attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard attach-policy *policy-name*

no ipv6 dhcp guard attach-policy

Parameters

- ***policy-name***—The DHCPv6 Guard policy name (up to 32 characters).

Default Configuration

The DHCPv6 Guard default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach a DHCPv6 Guard policy to a VLAN.

If a policy specified by the **policy-name** argument is not defined, the command is rejected.

Use the **no** form of the command to detach the current policy and to re-attach the default policy. The the **no** form of the command has no effect if the default policy was attached.

Example

In the following example, the DHCPv6 Guard policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 dhcp guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 dhcp guard policy

To define a DHCP Guard policy and place the switch in DHCPv6 Guard Policy Configuration mode, use the **ipv6 dhcp guard policy** command in Global Configuration mode. To remove the DHCPv6 guard policy, use the **no** form of this command.

Syntax

ipv6 dhcp guard policy *policy-name*

no ipv6 dhcp guard policy *policy-name*

Parameters

- ***policy-name***—The DHCPv6 Guard policy name (up to 32 characters).

Default Configuration

No DHCPv6 Guard policy are configured

Command Mode

Global Configuration mode

User Guidelines

This command defines the DHCPv6 Guard policy name, and places the router in DHCPv6 Guard Policy Configuration mode.

Each policy of the same type (for example, DHCPv6 Guard policies) must have a unique name. Policies of different types can have the same policy name.

The switch supports two predefined, default DHCPv6 Guard policies named: "vlan_default" and "port_default":

```
ipv6 dhcp guard policy vlan_default
      exit
      ipv6 dhcp guard policy port_default
      exit
```

The default policies are empty and cannot be removed, but can be changed. The **no ipv6 dhcp guard policy** does not remove the default policies, it only removes the policy configuration defined by the user.

You can define a policy using the **ipv6 dhcp guard policy** command multiple times.

Before an attached policy is removed, a request for confirmation is presented to the user, as shown in Example 3 below.

Example 1—The following example defines a DHCPv6 Guard policy named policy1, places the router in DHCPv6 Guard Policy Configuration mode, configures the port to drop unsecure messages and sets the device role as router:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

Example 2—The following example defines a DHCPv6 Guard named policy1 by multiple steps:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# device-role server
switchxxxxxx(config-dhcp-guard)# exit
```

Example 3—The following example removes an attached DHCPv6 Guard policy:

```
switchxxxxxx(config)# no ipv6 dhcp guard policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 dhcp guard preference

To globally enable verification of the preference in messages sent by DHCPv6 servers, use the **ipv6 dhcp guard preference** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 dhcp guard preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 dhcp guard preference [maximum] [minimum]

Parameters

- **maximum** *value*—Advertised preference value is lower than or equal to the **value** argument. Range 0-255. The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum** *value*—Advertised preference value is greater than or equal to the **value** argument. Range 0-255.

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification that the preference value in messages sent by DHCPv6 servers messages (see RFC3315) is greater than or less than the *value* argument.

Note. When DHCPv6 Guard receives a RELAY-REPL message, it takes it from the encapsulated message.

Configuring the **minimum** *value* keyword and argument specifies the minimum allowed value. The received DHCPv6 reply message with a preference value less than a value specified by the **value** argument is dropped.

Configuring the **maximum** *value* keyword and argument specifies the maximum allowed value. The received DHCPv6 reply message with a preference value greater than the value specified by the **value** argument is dropped.

Use **no ipv6 dhcp guard preference** to disable verification of the advertised preference value in DHCPv6 reply messages.

Use **no ipv6 dhcp guard preference maximum** to disable verification of the maximum boundary of the value of the advertised preference value in DHCPv6 messages.

Use the **no ipv6 dhcp guard preference minimum** command to disable verification of the minimum boundary of the value of the advertised preference value in DHCPv6 messages.

Example 1—The following example defines a global minimum preference value of 10 and a global maximum preference value of 102 using two commands:

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10
switchxxxxxx(config)# ipv6 dhcp guard preference maximum 102
```

Example 2—The following example defines a global minimum preference value of 10 and a global maximum preference value of 102 using a single command:

```
switchxxxxxx(config)# ipv6 dhcp guard preference minimum 10 maximum 102
```

ipv6 first hop security

To globally enable IPv6 First Hop Security on a VLAN, use the **ipv6 first hop security** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security

no ipv6 first hop security

Default Configuration

IPv6 First Hop Security on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the **ipv6 first hop security** command to enable IPv6 First Hop Security on a VLAN.

Example 1—The following example enables IPv6 First Hop Security on VLAN 100:

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 first hop security**

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

Example 2—The following example enables IPv6 First Hop Security on VLANs 100-107:

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 first hop security**

switchxxxxxx(config-if-range)# **exit**

ipv6 first hop security attach-policy (port mode)

To attach an IPv6 First Hop Security policy to a specific port, use the **ipv6 first hop security attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 first hop security attach-policy [*policy-name*]

Parameters

- ***policy-name***—The IPv6 First Hop Security policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the IPv6 First Hop Security policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which IPv6 First Hop Security is enabled.

Default Configuration

The IPv6 First Hop Security default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach an IPv6 First Hop Security policy to a port.

Each succeeding usage of this command overrides the previous usage of the command with the same policy.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 first hop security attach-policy** command to detach all user-defined policies attached to the port. The default policy is reattached.

Use the **no ipv6 first hop security attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the IPv6 First Hop Security policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the IPv6 First Hop Security policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the IPv6 First Hop Security policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the IPv6 First Hop Security policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example the IPv6 First Hop Security policy policy1 is detached from gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security attach-policy (VLAN mode)

To attach an IPv6 First Hop Security policy to a specified VLAN, use the **ipv6 first hop security attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security attach-policy *policy-name*

no ipv6 first hop security attach-policy

Parameters

- ***policy-name***—The IPv6 First Hop Security policy name (up to 32 characters).

Default Configuration

The IPv6 First Hop Security default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach an IPv6 First Hop Security policy to a VLAN.

If a policy specified by the **policy-name** argument is not defined, the command is rejected.

Use the **no** form of the command to return to detach the current policy and to reattach the default policy. The **no** form of the command does not have an effect if the default policy was attached.

Example

In the following example, the IPv6 First Hop Security policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 first hop security attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 first hop security logging packet drop

To globally enable the logging of dropped packets by the IPv6 First Hop Security feature, use the **ipv6 first hop security logging packet drop** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 first hop security logging packet drop

no ipv6 first hop security logging packet drop

Default Configuration

Logging is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use this command to log packets that are dropped. If logging is enabled, the switch sends a rate-limited SYSLOG message every time it drops a message.

Example

The following example shows how to enable logging of dropped packets by the IPv6 first-hop security feature:

```
switchxxxxxx(config)# ipv6 first hop security logging packet drop
```

ipv6 first hop security policy

To define an IPv6 First Hop Security policy and place the switch in IPv6 First Hop Security Policy Configuration mode, use the **ipv6 first hop security policy** command in Global Configuration mode. To remove the IPv6 First Hop Security policy, use the **no** form of this command.

Syntax

ipv6 first hop security policy *policy-name*

no ipv6 first hop security policy *policy-name*

Parameters

- ***policy-name***—The IPv6 First Hop Security policy name (up to 32 characters).

Default Configuration

No IPv6 First Hop Security policy is configured

Command Mode

Global Configuration mode

User Guidelines

This command defines an IPv6 First Hop Security policy, and places the switch in IPv6 First Hop Security Policy Configuration mode. Each policy of the same type (for example, IPv6 First Hop Security policies) must have a unique name. Policies of different types can have the same policy name. The switch supports two predefined, empty, default IPv6 First Hop Security policies named: "vlan_default" and "port_default":

```
ipv6 first hop security policy vlan_default
      exit
      ipv6 first hop security policy port_default
      exit
```

These policies cannot be removed but they can be changed. The **no ipv6 first hop security policy** does not remove these policies, it only removes the policy configurations defined by the user.

You can define a policy using the **ipv6 first hop security policy** command multiple times.

If an attached policy is removed, it is detached automatically before removing.

Examples

Example 1—The following example defines the IPv6 First Hop Security policy named policy1, places the switch in IPv6 First Hop Security Policy Configuration mode, and enables logging of dropped packets:

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config)# exit
```

Example 2—The following example removes an attached IPv6 First Hop Security policy:

```
switchxxxxxx(config)# no ipv6 first hop security policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy1 will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection

To enable the IPv6 Neighbor Discovery (ND) Inspection feature on a VLAN, use the **ipv6 nd inspection** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection

no ipv6 nd inspection

Default Configuration

ND Inspection on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the command to enable ND Inspection on a VLAN. The IPv6 ND Inspection validates the Neighbor Discovery Protocol (NDP) messages using the ND Inspection policies and global ND Inspection configuration. The ND Inspection bridges NDP messages to all ports excluding the source port within the VLAN with the following exception: RS and CPS messages are not bridged to ports configured as host (see the **device-role** command). The ND inspection is performed after RA Guard.

Example 1—The following example enables ND Inspection on VLAN 100:

switchxxxxxx(config)# **interface vlan** 100

switchxxxxxx(config-if)# **ipv6 nd inspection**

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

Example 2—The following example enables ND Inspection on VLANs 100-107:

switchxxxxxx(config)# **interface range vlan** 100-107

switchxxxxxx(config-if-range)# **ipv6 nd inspection**

switchxxxxxx(config-if-range)# **exit**

ipv6 nd inspection attach-policy (port mode)

To attach an ND Inspection policy to a specific port, use the **ipv6 nd inspection attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd inspection attach-policy [*policy-name*]

Parameters

- ***policy-name***—The ND Inspection policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the ND Inspection policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which ND Inspection is enabled.

Default Configuration

The ND Inspection default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **ipv6 nd inspection attach-policy** command to attach an ND Inspection policy to a port.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 nd inspection attach-policy** command to detach all user-defined policies attached to the port.

Use the **no ipv6 nd inspection attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the ND Inspection policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the ND Inspection policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the ND Inspection policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the ND Inspection policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example, ND Inspection detaches policy policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection attach-policy (VLAN mode)

To attach an ND Inspection policy to a specified VLAN, use the **ipv6 nd inspection attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection attach-policy *policy-name*

no ipv6 nd inspection attach-policy

Parameters

- ***policy-name***—The ND Inspection policy name (up to 32 characters).

Default Configuration

The ND Inspection default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach a ND Inspection policy to a VLAN. If the policy specified by the **policy-name** argument is not defined, the command is rejected. Use the **no** form of the command to detach the current policy and to reattach the default policy. The **no** form of the command does not have an effect if the default policy was attached.

Example

In the following example, the ND Inspection policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd inspection attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd inspection drop-unsecure

To globally enable dropping messages with no CGA and RSA Signature options, use the **ipv6 nd inspection drop-unsecure** command in Global Configuration mode. To disable this function, use the **no** form of this command.

Syntax

ipv6 nd inspection drop-unsecure

no ipv6 nd inspection drop-unsecure

Default Configuration

All messages are bridged.

Command Mode

Global Configuration mode

User Guidelines

This command drops NDP messages if they do not contain CGA and RSA Signature options.

If this command is not configured, then the **sec-level minimum** command does not have an effect.

If this command is configured, then only the **sec-level minimum** command has an effect and all other configured ND Inspection policy commands are ignored.

Example

The following example enables the switch to drop messages with no or invalid options or an invalid signature:

```
switchxxxxxx(config)# ipv6 nd inspection drop-unsecure
```

ipv6 nd inspection policy

To define an ND Inspection policy and place the switch in IPv6 ND Inspection Policy Configuration mode, use the **ipv6 nd inspection policy** command in Global Configuration mode. To remove the ND Inspection policy, use the **no** form of this command.

Syntax

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

Parameters

- ***policy-name***—The ND Inspection policy name (up to 32 characters).

Default Configuration

No ND Inspection policies are configured.

Command Mode

Global Configuration mode

User Guidelines

This command defines the ND Inspection policy name, and places the router in ND Inspection Policy Configuration mode. Each policy of the same type (for example, ND Inspection policies) must have a unique name. Policies of different types can have a same policy name.

The switch supports two predefined ND Inspection policies named: "vlan_default" and "port_default":

```
ipv6 nd inspection policy vlan_default
      exit
      ipv6 nd inspection policy port_default
      exit
```

These policies cannot be removed, but they can be changed. The **no ipv6 nd inspection policy** does not remove these policies, it only removes the policy configuration defined by the user.

You can define a policy using the **ipv6 nd inspection policy** command multiple times.

If an attached policy is removed it is detached automatically before removing.

Example 1. The following example defines a ND Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and configures the port to drop unsecured messages and sets the device role as router:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

Example 2. The following example defines an ND Inspection policy as policy1 by a few steps:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# drop-unsecure
switchxxxxxx(config-nd-inspection)# exit
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# device-role router
switchxxxxxx(config-nd-inspection)# exit
```

Example 3. The following example removes an attached ND Inspection policy:

```
switchxxxxxx(config)# no ipv6 nd inspection policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd inspection sec-level minimum

To globally specify the minimum security level value, use the **ipv6 nd inspection sec-level minimum** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd inspection sec-level minimum *value*

no ipv6 nd inspection sec-level minimum

Parameters

- ***value***—Sets the minimum security level. Range: 0–7.

Default Configuration

All messages are bridged.

Command Mode

Global Configuration mode

User Guidelines

This command specifies the minimum security level parameter value when the drop-unsecured feature is configured.

This command has no effect if dropping of non secure messages is disabled.

Example

The following example enables the switch to specify 2 as the minimum CGA security level:

```
switchxxxxxx(config)# ipv6 nd inspection sec-level minimum 2
```

ipv6 nd inspection validate source-mac

To globally enable checking source MAC address against the link-layer address in the source/target link-layer option, use the **ipv6 nd inspection validate source-mac** command in Global Configuration mode. To disable this function, use the **no** form of this command.

Syntax

ipv6 nd inspection validate source-mac

no ipv6 nd inspection validate source-mac

Parameters

N/A

Default Configuration

This command is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

When the switch receives an NDP message, which contains a link-layer address in the source/target link layer option, the source MAC address is checked against the link-layer address. Use this command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Example

The following example enables the switch to drop an NDP message whose link-layer address in the source/target link-layer option does not match the MAC address:

```
switchxxxxxx(config)# ipv6 nd inspection validate source-mac
```

ipv6 nd raguard

To globally enable the Router Advertisements (RA) guard feature on a VLAN, use the **ipv6 nd raguard** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard

no ipv6 nd raguard

Parameters

N/A

Default Configuration

RA Guard on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use the **ipv6 nd raguard** command, to enable IPv6 RA Guard on a VLAN. The RA Guard discards RA, CPA, and ICMP Redirect messages received on ports that are not configured as router (see the **device-role** command). The RA Guard validates received RA messages based on an RA Guard policy attached to the source port.

RA Guard is performed before ND inspection.

Example 1—The following example enables RA Guard on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables RA Guard on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 nd raguard
switchxxxxxx(config-if-range)# exit
```

ipv6 nd raguard attach-policy (port mode)

To attach an RA Guard policy to a specific port, use the **ipv6 nd raguard attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 nd raguard attach-policy [*policy-name*]

Parameters

- ***policy-name***—The RA Guard policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the RA Guard policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which RA Guard policy is enabled.

Default Configuration

The RA Guard default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach an RA Guard policy to a port. Each time the command is used, it overrides the previous command within the same policy. If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 nd raguard attach-policy** command to detach all user-defined policies attached to the port.

Use the no **ipv6 nd raguard attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the RA Guard policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the RA Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the RA Guard policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and the RA Guard policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example RA Guard detaches policy policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard attach-policy (VLAN mode)

To attach an RA Guard policy to a specified VLAN, use the **ipv6 nd raguard attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard attach-policy *policy-name*

no ipv6 nd raguard attach-policy

Parameters

- ***policy-name***—The RA Guard policy name (up to 32 characters).

Default Configuration

The RA Guard default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach an RA Guard policy to a VLAN.

If a policy specified by the **policy-name** argument is not defined, the command is rejected.

Use the **no** form of the command to detach the current policy and to reattach the default policy. The **no** form of the command has no effect if the default policy was attached.

Example

In the following example, the RA Guard policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 nd raguard attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 nd raguard hop-limit

To globally enable verification of the advertised Cur Hop Limit value in RA messages, use the **ipv6 nd raguard hop-limit** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard hop-limit {[maximum *value*] [minimum *value*]}

no ipv6 nd raguard hop-limit [maximum] [minimum]

Parameters

- **maximum** *value*—Verifies that the hop-count limit is lower than or equal to the **value** argument. Range 1-255. The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum** *value*—Verifies that the hop-count limit is greater than or equal to the **value** argument. Range 1-255.

Default Configuration

No hop-count limit is verified.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification that the advertised Cur Hop Limit value in an RA message (see RFC4861) is greater than or less than the value set by the **value** argument.

Configuring the **minimum** *value* keyword and argument can prevent an attacker from setting a low Cur Hop Limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised Cur Hop Limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *value* keyword and argument enables verification that the advertised Cur Hop Limit value is less than or equal to the value set by the **value** argument. If the advertised Cur Hop Limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Use the **no ipv6 nd raguard hop-limit maximum** command to disable verification of the maximum boundary of the advertised Cur Hop Limit value in an RA message.

Use the **no ipv6 nd raguard hop-limit minimum** command to disable verification of the minimum boundary of the advertised Cur Hop Limit value in an RA message.

Example 1—The following example defines a minimum Cur Hop Limit value of 3 and a maximum Cur Hop Limit value of 100 using two commands:

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3
switchxxxxxx(config)# ipv6 nd raguard hop-limit maximum 100
```

Example 2—The following example defines a minimum Cur Hop Limit value of 3 and a maximum Cur Hop Limit value of 100 using a single command:

```
switchxxxxxx(config)# ipv6 nd raguard hop-limit minimum 3 maximum 100
```

ipv6 nd raguard managed-config-flag

To globally enable verification of the advertised the Managed Address Configuration flag in RA messages, use the **ipv6 nd raguard managed-config-flag** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard managed-config-flag {on | off}

no ipv6 nd raguard managed-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification of the advertised the Managed Address Configuration flag (or the M flag) in an RA message (see RFC4861). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that might not be trustworthy.

Example

The following example enables M flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard managed-config-flag off
```

ipv6 nd raguard other-config-flag

To globally enable verification of the advertised “Other Configuration” flag in RA messages, use the **ipv6 nd raguard other-config-flag** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard other-config-flag {on | off}

no ipv6 nd raguard other-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification of the advertised “Other Configuration” flag (or "O" flag) in an RA message (see RFC4861). This flag could be set by an attacker to force hosts to retrieve other configuration information through a DHCPv6 server that might not be trustworthy.

Example

The following example shows how the command enables O flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard other-config-flag off
```

ipv6 nd raguard policy

To define an RA Guard policy name and place the switch in IPv6 RA Guard Policy Configuration mode, use the **ipv6 nd raguard policy** command in Global Configuration mode. To remove the RA Guard policy, use the **no** form of this command.

Syntax

ipv6 nd raguard policy *policy-name*

no ipv6 nd raguard policy *policy-name*

Parameters

- ***policy-name***—The RA Guard policy name (up to 32 characters).

Default Configuration

No RA Guard policy is configured

Command Mode

Global Configuration mode

User Guidelines

This command defines the RA Guard policy name, and places the switch in IPv6 RA Guard Policy Configuration mode.

Each policy of the same type (for example, RA Guard policies) must have a unique name. Policies of different types can have a same policy name.

The switch supports two predefined RA Guard policies, named: "vlan_default" and "port_default":

```
ipv6 nd raguard policy vlan_default
exit
ipv6 nd raguard policy port_default
exit
```

The policies cannot be removed, but they can be changed. The **no ipv6 nd raguard policy** does not remove these policies, it only removes the policy configuration defined by the user.

The **vlan_default** policy is attached by default to a VLAN, if no other policy is attached to the VLAN. The **port_default** policy is attached by default to a port, if no other policy is attached to the port.

You can define a policy using the **ipv6 nd raguard policy** command multiple times. If an attached policy is removed, it is detached automatically before removing.

Example 1—The following example defines an RA Guard policy named policy1, places the router in RA Guard Policy Configuration mode, and disenabled validation of the Other Configuration flag, and sets the device role as router:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

Example 2—The following example defines an RA Guard named policy1 using multiple steps:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag disable
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# device-role router
switchxxxxxx(config-ra-guard)# exit
```

Example 3—The following example removes an attached RA Guard policy:

```
switchxxxxxx(config)# no ipv6 nd raguard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2
```

```
The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 nd raguard router-preference

To globally enable verification of the advertised Default Router Preference value in RA messages, use the **ipv6 nd raguard router-preference** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 nd raguard router-preference {[**maximum** *value*] [**minimum** *value*]}

no ipv6 nd raguard router-preference [maximum] [minimum]

Parameters

- **maximum** *value*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191). The value of the high boundary must be equal to or greater than the value of the low boundary.
- **minimum** *value*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191).

Default Configuration

Verification is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables verification of the advertised Default Router Preference value in RA messages (see RFC4191).

Configuring the **minimum** *value* keyword and argument specifies the minimum allowed value. Received RA messages with a Default Router Preference value less than the *value* argument are dropped.

Configuring the **maximum** *value* keyword and argument specifies the maximum allowed value. Received RA messages with a Default Router Preference value greater than the *value* argument are dropped.

Use the **no ipv6 nd raguard router-preference** command to disable verification of the advertised Default Router Preference value in RA messages.

Use the **no ipv6 nd raguard router-preference maximum** command to disable verification of the maximum boundary of the advertised Default Router Preference value in RA messages.

Use the **no ipv6 nd raguard router-preference minimum** command to disable verification of the advertised Default Router Preference value in RA messages.

Example 1—The following example defines that only a value of **medium** is acceptable using two commands:

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium
switchxxxxxx(config)# ipv6 nd raguard router-preference maximum medium
```

Example 2—The following example defines that only a value of **medium** is acceptable using a single command:

```
switchxxxxxx(config)# ipv6 nd raguard router-preference minimum medium maximum medium
```

ipv6 neighbor binding

To globally enable the Neighbor Binding (NB) integrity feature on a VLAN, use the **ipv6 neighbor binding** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding

no ipv6 neighbor binding

Parameters

N/A

Default Configuration

NB integrity on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

NB integrity establishes binding for neighbors connected to the perimetrical ports belonging to the VLANs on which the feature is enabled.

Example 1—The following example enables NB integrity on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables NB integrity on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 neighbor binding
switchxxxxxx(config-if-range)# exit
```

ipv6 neighbor binding address-config

To specify allowed configuration methods of global IPv6 addresses, use the **ipv6 neighbor binding address-config** command in Global Configuration mode. To return to the default setting, use the **no** form of this command.

Syntax

ipv6 neighbor binding address-config [stateless | any] [dhcp]

no ipv6 neighbor binding address-config

Parameters

- **stateless**—Only auto configuration is allowed for global IPv6 bound from NDP messages.
- **any**—All configuration methods for global IPv6 bound from NDP messages (stateless and manual) are allowed. If no keyword is defined the **any** keyword is applied.
- **dhcp**—Binding from DHCPv6 is allowed.

Default Configuration

Any is the default parameter.

Command Mode

Global Configuration mode

User Guidelines

This command defines allowed IPv6 address configuration methods for global IPv6 addresses.

The **stateless** and **any** keywords specify the following:

- Global IPv6 addresses are bound from NDP messages. If none of these keywords are configured, only link-local addresses are bound from NDP messages.
- How global IPv6 addresses, bound from NDP messages, are checked against the Neighbor Prefix table, if prefix validation is enabled:

  stateless—IPv6 addresses are bound from NDP messages, and only global addresses belonging to learned prefixes with set A-flag or prefixes manually configured with the **autoconfig** keyword are allowed.

  any—IPv6 addresses are bound from NDP messages and only global addresses belonging to prefixes in NPT are allowed.

Use the **dhcp** keyword, to allow binding from DHCPv6 message. IPv6 addresses bound from DHCPv6 messages are never verified against the Neighbor Prefix table. IPv6 addresses bound from DHCPv6 messages override IPv6 addresses bound from NDP messages.

Note. If the **dhcp** keyword is not configured, the switch will bind IPv6 addresses assigned by DHCPv6 from NDP messages, because a host must execute the DAD process for these addresses.

If no keyword is defined the **ipv6 neighbor binding address-config any** command is applied.

Example 1. The following example specifies that any global IPv6 address configuration method can be applied and there will be no binding from DHCPv6 messages:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any
```

Example 2. The following example specifies that any global IPv6 address binding from NDP and global IPv6 address binding from DHCPv6 messages can be applied:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config any dhcp
```

Example 3. The following example specifies that only stateless global IPv6 address binding from NDP can be applied

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless
```

Example 4. The following example specifies that only the stateless IPv6 address configuration and assignment by DHCPv6 methods can be applied and binding only from NDP messages is supported:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
switchxxxxxx(config)# ipv6 neighbor binding address-config stateless dhcp
```

Example 5. The following example specifies that global IPv6 addresses can be assigned only by DHCPv6:

```
switchxxxxxx(config)# ipv6 neighbor binding address-config dhcp
```

ipv6 neighbor binding address-prefix

To define a static prefix for global IPv6 addresses bound from NDP messages, use the **ipv6 neighbor binding address-prefix** command in Global Configuration mode. To delete the prefix, use the **no** form of this command.

Syntax

ipv6 neighbor binding address-prefix vlan *vlan-id ipv6-prefix*/*prefix-length* [**autoconfig**]

no ipv6 neighbor binding address-prefix [vlan *vlan-id*] [*ipv6-prefix*/*prefix-length*]

Parameters

- ***ipv6-prefix***/*prefix-length*—IPv6 prefix.
- **vlan** *vlan-id*—ID of the specified VLAN.
- **autoconfig**—The prefix can be used for stateless configuration.

Default Configuration

No static prefix

Command Mode

Global Configuration mode

User Guidelines

Use the **ipv6 neighbor binding address-prefix** command to add a static prefix to the Neighbor Prefix table.

Use the **no ipv6 neighbor binding address-prefix vlan** *vlan-id ipv6-prefix*/*prefix-length* command to remove one static entry from the Neighbor Prefix table.

Use the **no ipv6 neighbor binding address-prefix vlan** *vlan-id* command to remove all static entries from the Neighbor Prefix table defined on the given VLAN.

Use the **no ipv6 neighbor binding address-prefix** command to remove all static entries from the Neighbor Prefix table.

Example 1. The following example adds two static entries. The second one can be used for stateless configuration.

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:100::/64
autoconfig
```

Example 2. The following example deletes a single static entry:

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100 2001:0DB8:101::/64
```

Example 3. The following example deletes all static entries defined on the specified VLAN:

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix vlan 100
```

Example 4. The following example deletes all static entries:

```
switchxxxxxx(config)# no ipv6 neighbor binding address-prefix
```

ipv6 neighbor binding address-prefix-validation

To globally enable validation of a bound IPv6 address against the Neighbor Prefix table, use the **ipv6 neighbor binding address-prefix-validation** command in Global Configuration mode. To disable this feature, use the **no** form of this command.

Syntax

ipv6 neighbor binding address-prefix-validation

no ipv6 neighbor binding address-prefix-validation

Parameters

N/A

Default Configuration

The feature is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables bound address prefix validation. If the Neighbor Binding feature is enabled, the switch checks if a bound address belongs to one of the prefixes of the Neighbor Prefix table or to a manually-configured prefix list by the command in the Neighbor Binding configuration mode. If an address does not belong, it is not bound.

Example

The following example shows how to enable bound address validation against the Neighbor Prefix table:

```
switchxxxxxx(config)# ipv6 neighbor binding address-prefix-validation
```

ipv6 neighbor binding attach-policy (port mode)

To attach a Neighbor Binding policy to a specific port, use the **ipv6 neighbor binding attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding attach-policy *policy-name* [**vlan** *vlan-list*]

no ipv6 neighbor binding attach-policy [*policy-name*]

Parameters

- ***policy-name***—The Neighbor Binding policy name (up to 32 characters).
- **vlan** *vlan-list*—Specifies that the Neighbor Binding policy is to be attached to the VLAN(s) in *vlan-list*. If the **vlan** keyword is not configured, the policy is applied to all VLANs on the device on which Neighbor Binding policy is enabled.

Default Configuration

The Neighbor Binding default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach a Neighbor Binding policy to a port.

Each time the command is used, it overrides the previous command within the same policy.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Multiple policies with the **vlan** keyword can be attached to the same port if they do not have common VLANs.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port on the VLAN on which the packet arrived are added to the set.
- The rules, configured in the policy attached to the VLAN are added to the set if they have not been added.
- The global rules are added to the set if they have not been added.

Use the **no ipv6 neighbor binding attach-policy** command to detach all user-defined policies attached to the port.

Use the **no ipv6 neighbor binding attach-policy** *policy-name* command to detach the specific policy from the port.

Example 1—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10 and 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10,12-20
switchxxxxxx(config-if)# exit
```

Example 3—In the following example, the Neighbor Binding policy policy1 is attached to the gi1/0/1 port and applied to VLANs 1-10, and the Neighbor Binding policy policy2 is attached to the gi1/0/1 port and applied to VLANs 12-20:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1 vlan 1-10
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy2 vlan 12-20
switchxxxxxx(config-if)# exit
```

Example 4—In the following example, Neighbor Binding Integrity detaches policy policy1 detached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding attach-policy (VLAN mode)

To attach a Neighbor Binding policy to a specific VLAN, use the **ipv6 neighbor binding attach-policy** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding attach-policy *policy-name*

no ipv6 neighbor binding attach-policy

Parameters

- ***policy-name***—The Neighbor Binding policy name (up to 32 characters).

Default Configuration

The Neighbor Binding default policy is applied.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

Use this command to attach a Neighbor Binding policy to a VLAN.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

Use the **no** form of the command to return to detach the current policy and reattach the default policy. The **no** form of the command has no effect if the default policy was attached.

Example

In the following example, the Neighbor Binding policy policy1 is attached to VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 neighbor binding attach-policy policy1
switchxxxxxx(config-if)# exit
```

ipv6 neighbor binding lifetime

To globally change the default of the Neighbor Binding table entry lifetime, use the **ipv6 neighbor binding lifetime** command in Global Configuration mode. To return to the default setting, use the **no** form of this command.

Syntax

ipv6 neighbor binding lifetime *value*

no ipv6 neighbor binding lifetime

Parameters

- ***value***—The lifetime in minutes. The range is from 1 through 60 minutes.

Default Configuration

5 minutes

Command Mode

Global Configuration mode

User Guidelines

Use the **ipv6 neighbor binding lifetime** command to change the default lifetime.

Example

The following example changes the lifetime for binding entries to 10 minutes:

```
switchxxxxxx(config)# ipv6 neighbor binding lifetime 10
```

ipv6 neighbor binding max-entries

To globally specify the maximum number of dynamic entries that are allowed to be inserted in the Binding table cache, use the **ipv6 neighbor binding max-entries** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 neighbor binding max-entries {[**vlan-limit** *number*] [**interface-limit** *number*] [**mac-limit** *number*]}

no ipv6 neighbor binding max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

Parameters

- **vlan-limit** *number*—Specifies a neighbor binding limit per number of VLANs.
- **interface-limit** *number*—Specifies a neighbor binding limit per port.
- **mac-limit** *number*—Specifies a neighbor binding limit per MAC address.

Default Configuration

This command is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command is used to control the contents of the Binding table. This command specifies the maximum number of dynamic entries that can be inserted in the Binding table cache. After this limit is reached, new entries are refused, and a Neighbor Discovery Protocol (NDP) traffic source with a new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

Example

The following example shows how to specify globally the maximum number of entries that can be inserted into the cache per MAC:

```
switchxxxxxx(config)# ipv6 neighbor binding max-entries mac-limit 2
```

ipv6 neighbor binding policy

To define a Neighbor Binding policy and place the switch in IPv6 Neighbor Binding Policy Configuration mode, use the **ipv6 neighbor binding policy** command in Global Configuration mode. To remove the Neighbor Binding policy, use the **no** form of this command.

Syntax

ipv6 neighbor binding policy *policy-name*

no ipv6 neighbor binding policy *policy-name*

Parameters

- ***policy-name***—The Neighbor Binding policy name (up to 32 characters).

Default Configuration

No Neighbor Binding policy is configured

Command Mode

Global Configuration mode

User Guidelines

This command defines a Neighbor Binding policy name, and places the router in Neighbor Binding Policy Configuration mode so that additional commands can be added to the policy.

The switch supports two predefined Neighbor Binding policies, named: "vlan_default" and "port_default":

```
ipv6 neighbor binding policy vlan_default
      exit
      ipv6 neighbor binding policy port_default
      exit
```

The policies cannot be removed, but they can be changed. The **no ipv6 neighbor binding policy** does not remove these policies, it only removes the policy configuration defined by the user.

You can define a policy using the **ipv6 neighbor binding policy** command multiple times.

If an attached policy is removed, it is detached automatically before removing.

Example 1—The following example defines a Neighbor Binding policy named policy1, places the router in Neighbor Binding Policy Configuration mode, enables logging, and defines the port as internal:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# logging binding
switchxxxxxx(config-nbr-binding)# exit
```

Example 2—The following example defines a Neighbor Binding policy named policy1 using multiple steps:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# device-role internal
switchxxxxxx(config-nbr-binding)# exit
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
logging binding
witchxxxxxx(config-nbr-binding)# exit
```

Example 3—The following example remove an attached Neighbor Binding policy:

```
switchxxxxxx(config)# no ipv6 neighbor binding policy policy1
Policy policy1 is applied on the following ports:
 gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

ipv6 neighbor binding static

To add a static entry to the Neighbor Binding table, use the **ipv6 neighbor binding static** command in Global Configuration mode. To remove the static entry, use the **no** form of this command.

Syntax

ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id* **interface** *interface-id* **mac** *mac-address*

no ipv6 neighbor binding static ipv6 *ipv6-address* **vlan** *vlan-id*

Parameters

- **ipv6** *ipv6-address*—IPv6 address of the static entry.
- **vlan** *vlan-id*—ID of the specified VLAN.
- **interface** *interface-id*—Adds static entries to the specified port.
- **mac** *mac-address*—MAC address of the static entry.

Default Configuration

No static entry.

Command Mode

Global Configuration mode

User Guidelines

This command is used to add static entries to the Neighbor Binding table. Static entries can be configured regardless the port role.

If the entry (dynamic or static) already exists, the new static entry overrides the existing one.

If the Neighbor Binding table overflows, the static entry is not added.

Example

The following example adds a static entry:

```
switchxxxxxx(config)# ipv6 neighbor binding static ipv6 2001:600::1 vlan 100 interface
gi1/0/1 mac 00BB.CC01.F500
```

ipv6 source guard

To enable the IPv6 Source Guard feature on a VLAN, use the **ipv6 source guard** command in VLAN Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 source guard

no ipv6 source guard

Default Configuration

Source Guard on a VLAN is disabled.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

IPv6 Source Guard blocks an IPv6 data message arriving on a port if its source IPv6 address is bound to another port, or it is unknown.

Example 1—The following example enables IPv6 Source Guard on VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 source guard
switchxxxxxx(config-if)# exit
```

Example 2—The following example enables IPv6 Source Guard on VLANs 100-107:

```
switchxxxxxx(config)# interface range vlan 100-107
switchxxxxxx(config-if-range)# ipv6 source guard
switchxxxxxx(config-if-range)# exit
```

ipv6 source guard attach-policy (port mode)

To attach an IPv6 Source Guard policy to a specific port, use the **ipv6 source guard attach-policy** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 source guard attach-policy *policy-name*

no ipv6 source guard attach-policy

Parameters

- ***policy-name***—The IPv6 Source Guard policy name (up to 32 characters).

Default Configuration

The IPv6 Source Guard default policy is applied.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to attach an IPv6 Source Guard policy to a port.

Each succeeding **ipv6 source guard attach-policy** command overrides the previous policy attachment on the same port.

IPv6 Source guard policies can be used to block forwarding IPv6 data messages with unknown source IPv6 addresses or with source IPv6 addresses bound to a port differing from the input one.

If a policy specified by the *policy-name* argument is not defined, the command is rejected.

The set of rules that is applied to an input packet is built in the following way:

- The rules, configured in the policy attached to the port.
- The global rules are added to the set if they have not been added.

Use the no ipv6 source guard attach-policy command to detach the user defined policy attached to the port and to reattach the default policy with name "port_default".

Example 1—In the following example, the IPv6 Source Guard policy policy1 is attached to the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# ipv6 source guard attach-policy policy1
switchxxxxxx(config-if)# exit
```

Example 2—In the following example IPv6 Source Guard detaches policy1 from the gi1/0/1 port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no ipv6 source guard attach-policy
switchxxxxxx(config-if)# exit
```

ipv6 source guard policy

To define an IPv6 Source Guard policy name and place the user in IPv6 Source Guard Configuration, use the **ipv6 source guard policy** command in Global Configuration mode. To remove the IPv6 Source Guard policy name, use the **no** form of this command.

Syntax

ipv6 source guard policy *policy-name*

no ipv6 source guard policy *policy-name*

Parameters

- ***policy-name***—The IPv6 Source Guard policy name (up to 32 characters).

Default Configuration

No IPv6 Source Guard policies are configured.

Command Mode

Global Configuration mode

User Guidelines

This command defines the IPv6 Source Guard policy name, and places the router in IPv6 Source Guard Policy Configuration mode.

Each policy of the same type (for example, IPv6 Source Guard policies) must have a unique name. Policies of different types can have the same policy name.

The switch supports one predefined IPv6 Source Guard policy named: "port_default":

```
ipv6 source guard policy port_default
      exit
```

The policy cannot be removed, but it can be changed. The **no ipv6 source guard policy** does not remove the policy, it only removes any policy configurations defined by the user.

If an attached policy is removed, it is detached automatically before removing.

Example 1—The following example defines the IPv6 Source Guard policy named policy1, places the router in IPv6 Source Guard Policy Configuration mode, and configures the port as trusted:

```
switchxxxxxx(config)# ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config)# exit
```

Example 2—The following example removes the attached IPv6 Source Guard policy:

```
switchxxxxxx(config)# no ipv6 source guard policy policy1
Policy policy1 is applied on the following ports:
gi1/0/1, gi1/0/2

The policy will be detached and removed, are you sure [Y/N]Y
```

logging binding

To enable the logging of Binding table main events within an IPv6 Neighbor Binding policy, use the **logging binding** command in Neighbor Binding Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

logging binding [enable | disable]

no logging binding

Parameters

- **enable**—Enables logging of Binding table main events. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables logging of Binding table main events.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables logging of Binding table main events within the IPv6 Neighbor Binding policy named policy1:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# logging binding enable
switchxxxxxx(config-nbr-binding)# exit
```

logging packet drop

To enable the logging of dropped packets within an IPv6 First Hop Security policy, use the **logging packet drop** command in IPv6 First Hop Security Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

logging packet drop [enable | disable]

no logging packet drop

Parameters

- **enable**—Enables logging of dropped packets. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables logging of dropped packets.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

IPv6 First Hop Security Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables logging of dropped messaged with the IPv6 First Hop Security Policy named policy1:

```
switchxxxxxx(config)# ipv6 first hop security policy policy1
switchxxxxxx(config-ipv6-fhs)# logging packet drop
switchxxxxxx(config-ipv6-fhs)# exit
```

managed-config-flag

To enable verification of the advertised Managed Address Configuration flag within an IPv6 RA Guard policy, use the **managed-config-flag** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

managed-config-flag {on | off | disable}

no managed-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.
- **disable**—The value of the flag is not validated.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and enables M flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# managed-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

match ra address

To enable verification of the router's IPv6 address in received RA messages within an IPv6 RA Guard policy, use the **match ra address** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match ra address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra address

Parameters

- **prefix-list** *ipv6-prefix-list-name*—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the router's IPv6 address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: router's addresses are not verified.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

This command enables verification of the router's IPv6 address in received RA messages by a configured prefix list. If the router's source IPv6 address does not match the prefix list or if the prefix list is not configured, the RA message is dropped.

Use the **disable** keyword to disable verification of the router's IPv6 address regardless of the VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, matches the router addresses to the prefix list named list1, and defines the prefix list named list1 authorizing the router with link-local address FE80::A8BB:CCFF:FE01:F700 only:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra address prefix-list list1
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

match ra prefixes

To enable verification of the advertised prefixes in received RA messages within an IPv6 RA Guard policy, use the **match ra prefixes** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match ra prefixes {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match ra prefixes

Parameters

- **prefix-list** *ipv6-prefix-list-name*—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the advertised prefixes in received RA messages.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: advertised prefixes are not verified.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

This command enables verification of the advertised prefixes in received RA messages by a configured prefix list. If an advertised prefix does not match the prefix list, or if the prefix list is not configured, the RA message is dropped.

Use the **disable** keyword to disable verification of the advertised prefixes in received RA messages in both global or the VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard configuration mode, matches the prefixes to the prefix list named list1, and the 2001:101::/64 prefixes and denies 2001:100::/64 prefixes:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# match ra prefixes prefix-list list1
switchxxxxxx(config-ra-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:101::/64
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/64
```

match reply

To enable verification of the assigned IPv6 addressed in messages sent by DHCPv6 servers/relays to a configured prefix list within a DHCPv6 Guard policy, use the **match reply** command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match reply {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match reply

Parameters

- ***ipv6-prefix-list-name***—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the advertised prefixes in replies.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: advertised prefixes are not verified.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

IPv6 DHCP Guard verifies the assigned IPv6 addresses to the configure prefix list passed in the IA_NA and IA_TA options of the following DHCPv6 messages sent by DHCPv6 servers/relays:

- ADVERTISE
- REPLY
- RELAY-REPL

Note 1. Assigned addresses are not verified if a value of the Status Code option (if it presents) differs from the following ones:

- Success
- UseMulticast

Note 2. In RELAY-REPL messages DHCPv6 Guard validates the message encapsulated in the DHCP-relay-message option.

Use the **disable** keyword to disable verification of the assigned IPv6 addresses in replies.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard policy configuration mode, matches the assigned addresses to the prefix list named list1: all assigned IPv6 addresses must belong to 2001:0DB8:100:200/64 or to 2001:0DB8:100::/48. The **"ge 128"** parameter must be configured for each prefix of the prefix-list with prefix length less than 128.

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match reply prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 deny 2001:0DB8:100:200/64 ge 128
switchxxxxxx(config)# ipv6 prefix-list list1 permit 2001:0DB8:100::/48 ge 128
```

match server address

To enable verification of the source IPv6 address in messages sent by DHCPv6 servers or DHCPv6 Relays to a configured prefix list within a DHCPv6 Guard policy, use the **match server address** command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

match server address {**prefix-list** *ipv6-prefix-list-name*} | **disable**

no match server address

Parameters

- **prefix-list** *ipv6-prefix-list-name*—The IPv6 prefix list to be matched.
- **disable**—Disables verification of the DHCP server's and relay's IPv6 address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: server's addresses are not verified.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

This command enables verification of the source IPv6 address in messages sent by DHCPv6 servers and DHCPv6 Relays to a configured prefix list. If the source IPv6 address does not match the configured prefix list, or if the prefix list is not configured, the DHCPv6 reply is dropped.

IPv6 DHCP Guard verifies the source IPv6 address in the following DHCPv6 messages sent by DHCPv6 servers/relays:

- ADVERTISE
- REPLY
- RECONFIGURE
- RELAY-REPL
- LEASEQUERY-REPLY

Use the **disable** keyword to disable verification of the DHCP server's and relay's IPv6 address.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard Policy Configuration mode, matches the server or relay addresses to the prefix list named list1, and defines the prefix list named list1 authorizing the server with link-local address FE80::A8BB:CCFF:FE01:F700 only:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# match server address prefix-list list1
switchxxxxxx(config-dhcp-guard)# exit
switchxxxxxx(config)# ipv6 prefix-list list1 permit FE80::A8BB:CCFF:FE01:F700/128
```

max-entries

To define the maximum number of dynamic entries that can be inserted in the Binding table cache within an IPv6 Neighbor Binding policy, use the **max-entries** command in Neighbor Binding Policy Configuration mode.To return to the default, use the **no** form of this command.

Syntax

max-entries {[**vlan-limit** {*number* | **disable**}] [**interface-limit** {*number* | **disable**}] [**mac-limit** {*number* | **disable**}]}

no max-entries [**vlan-limit**] [**interface-limit**] [**mac-limit**]

Parameters

- **vlan-limit** *number*—Specifies a neighbor binding limit per VLANs. The parameter is ignored in a policy attached to port.
- **vlan-limit disable**—Disables a neighbor binding limit per VLANs.
- **interface-limit** *number*—Specifies a neighbor binding limit per port.
- **interface-limit disable**—Disables a neighbor binding limit per port.
- **mac-limit** *number*—Specifies a neighbor binding limit per MAC address.
- **mac-limit disable**—Disables a neighbor binding limit per MAC address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

Neighbor Binding Policy Configuration mode.

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example 1—The following example defines an Neighbor Binding policy named policy1, places the router in Neighbor Binding Policy Configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
switchxxxxxx(config)# ipv6 neighbor binding policy policy1
switchxxxxxx(config-nbr-binding)# max-entries interface-limit 25
switchxxxxxx(config)# exit
```

Example 2—The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and disables limit per MAC:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# max-entries mac-limit disable

switchxxxxxx(config-ra-guard)# exit
```

other-config-flag

To enable the verification of the advertised the Other Configuration flag in RA messages within an IPv6 RA Guard policy, use the **other-config-flag** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

other-config-flag {on | off | disable}

no other-config-flag

Parameters

- **on**—The value of the flag must be 1.
- **off**—The value of the flag must be 0.
- **disable**—The value of the flag is not validated.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

User Guidelines

Use the **disable** keyword to disable flag validation in both global or VLAN configuration.

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and enables O flag verification that checks if the value of the flag is 0:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# other-config-flag off
switchxxxxxx(config-ra-guard)# exit
```

preference

To enable verification of the preference in messages sent by DHCPv6 servers within a DHCPv6 Guard policy, use the **preference** command in DHCPv6 Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

preference {[**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]}

no preference [maximum] [minimum]

Parameters

- **maximum** *value*—Advertised preference value is lower or equal than that set by the value argument. Range 0-255. A value of the high boundary must be equal to or greater than a value of the low boundary.
- **maximum disable**—Disables verification of the high boundary of the advertised preference value.
- **minimum** *value*—Advertised preference value is greater than or equal to the **value** argument. Range 0-255.
- **minimum disable**—Disables verification of the lower boundary of the advertised preference value.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

DHCP Guard Policy Configuration mode

User Guidelines

Use the **disable** keyword to disable verification in both global or VLAN configuration.

Example

The following example defines a DHCPv6 Guard policy named policy1, places the switch in DHCPv6 Guard Policy Configuration mode, and defines a minimum preference value of 10:

```
switchxxxxxx(config)# ipv6 dhcp guard policy policy1
switchxxxxxx(config-dhcp-guard)# preference minimum 10
switchxxxxxx(config-dhcp-guard)# exit
```

router-preference

To enable verification of advertised Default Router Preference value in RA messages within an IPv6 RA Guard policy, use the **router-preference** command in RA Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

router-preference [**maximum** {*value* | **disable**}] [**minimum** {*value* | **disable**}]

no router-preference [maximum] [minimum]

Parameters

- **maximum** *value*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191). A value of the high boundary must be equal to or greater than a value of the low boundary.

- **maximum disable**—Disables verification of the high boundary of Advertised Default Router Preference.
- **minimum** *value*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: **low**, **medium** and **high** (see RFC4191).
- **minimum disable**—Disables verification of the low boundary of Advertised Default Router Preference.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

RA Guard Policy Configuration mode

Example

The following example defines an RA Guard policy named policy1, places the switch in RA Guard Policy Configuration mode, and defines a minimum Default Router Preference value of medium:

```
switchxxxxxx(config)# ipv6 nd raguard policy policy1
switchxxxxxx(config-ra-guard)# router-preference minimum medium
switchxxxxxx(config-ra-guard)# exit
```

sec-level minimum

To specify the minimum security level value within an Ipv6 ND Inspection policy, use the **sec-level minimum** command in ND Inspection policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

sec-level minimum *value* | disable

no sec-level minimum

Parameters

- ***value***—Sets the minimum security level, which is a value from 0 through 7.
- **disable**—Disables verification of security level parameter

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND inspection Policy Configuration mode

User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

This command has no effect if dropping of unsecured messages is disabled.

Example

The following example defines an NDP Inspection policy named policy1, places the switch in ND Inspection Policy Configuration mode, and specifies 2 as the minimum CGA security level:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# sec-level minimum 2
switchxxxxxx(config-nd-inspection)# exit
```

show ipv6 dhcp guard

To display DHCPv6 Guard global configuration, use the **show ipv6 dhcp guard** command in Privilege EXEC configuration mode.

Syntax

show ipv6 dhcp guard

Command Mode

Privileged EXEC mode

User Guidelines

The **show ipv6 dhcp guard** command displays DHCPv6 Guard global configuration.

Example

The following example gives an example of the output of the **show ipv6 dhcp guard** command:

```
switchxxxxxx# show ipv6 dhcp guard
IPv6 DHCP Guard is enabled on VLANs:1-4,6,7,100-120
Default Preference
  minimum: 10
  maximum: 100
```

show ipv6 dhcp guard policy

To display DHCPv6 guard policies on all ports configured with the DHCPv6 guard feature, use the **show ipv6 dhcp guard policy** command in privileged EXEC mode.

Syntax

show ipv6 dhcp guard policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the DHCPv6 guard policy with the given name.
- **active**—Displays the attached DHCPv6 guard policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the options configured for the policy on all ports configured with the DHCPv6 guard feature.

Example 1—The following example displays the Policy Configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 dhcp guard policy policy1
DHCPv6 Guard Policy: policy1
  device-role: server
  preference
    minimum: 1
    maximum: 200
  server address prefix list: list1
  reply prefix list name: list10
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 dhcp guard policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-2	1-100
	port-default	gi1/0/1-2	101-4094
		gi1/0/3-4	1-1094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 dhcp guard policy
policy1
policy2
```

show ipv6 first hop security

To display all IPv6 First Hop Security global configuration, use the **show ipv6 first hop security** command in Privilege EXEC configuration mode.

Syntax

show ipv6 first hop security

Command Mode

Privileged EXEC mode

User Guidelines

This command displays all IPv6 First Hop Security global configuration.

Example

The following example gives an example of the **show ipv6 first hop security** command:

```
switchxxxxxx# show ipv6 first hop security
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
Logging Packet Drop: enabled
```

show ipv6 first hop security active policies

To display information about the policies applied to the port and to the VLAN, use the **show ipv6 first hop security active policies** command in privileged EXEC mode.

Syntax

show ipv6 first hop security active policies interface *interface-id* vlan *vlan-id*

Parameters

- **interface** *interface-id*—Port Identifier (Ethernet port or port channel).
- **vlan** *vlan-id*—VLAN Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays policies applied to frames arriving on given port and belonging to the given VLAN. The policies are calculated automatically by using the policies attached to the port, VLAN, and the global configuration

Example

The following example displays the active attached policies on gi1/0/1 and VLAN 100:

```
switchxxxxxx# show ipv6 first hop security active policies interface gi1/0/1 vlan 100
IPv6 First Hop Security is enabled on VLANs:1-4,6,7,100-120
IPv6 DHCP Guard is enabled on VLANs:1-4
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
IPv6 Neighbor Binding Integrity is enabled on VLANs:1-4,6,7,100-120
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
IPv6 Source Guard is enabled on VLANs:1-3,7,100-112
gi1/0/1, VLAN 100
IPv6 First Hop Security Policy:
  logging packet drop: enabled (from global configuration)
DHCPv6 Guard Policy:
  device-role: server (from policy1 attached to the port)
  reply prefix list name: list10 (from policy2 attached to the VLAN)
  server address prefix list name: list22 (from policy2 attached to the VLAN)
  preference
    minimum: 1 (from policy2 attached to the VLAN)
    maximum: 200 (from policy2 attached to the VLAN)
ND Inspection Policy:
  device-role: host (default)
  drop-unsecure: enabled (from policy2 attached to the VLAN)
  sec-level minimum: 3 (from policy1 attached to the port)
  validate source-mac: enabled (from global configuration)
Neighbor Binding Policy: policy1
  device-role: perimiter (default)
  logging binding: enabled (from policy1 attached to the port)
  address-prefix-validation: enabled (from policy2 attached to the VLAN)
  address-config: any (default)
  maximum entries
   VLAN: unlimited (from global configuration)
   Port: 1 (from policy1 attached to the port)
   MAC: 2 (from policy2 attached to the VLAN)
RA Guard Policy:
  device-role: router (from policy1 attached to the port)
  hop-limit:
    minimum: 10 (from policy2 attached to the VLAN)
    maximum: 20 (from global configuration)
  manage-config-flag: on(from policy2 attached to the VLAN)
  ra address verification::  disabled(default)
  ra prefixes prefix list name: list1(from policy2 attached to the VLAN)
  other-flag: disabled (default)
  router-preference:
    minimum: medium (from policy2 attached to the VLAN)
    maximum: medium (from policy2 attached to the VLAN)
IPv6 Source Guard Policy:
  trusted port: enabled (from policy1 attached to the port)
```

show ipv6 first hop security attached policies

To display information about the policies attached to the port and to the VLAN, use the **show ipv6 first hop security attached policies** command in privileged EXEC mode.

Syntax

show ipv6 first hop security attached policies interface *interface-id* vlan *vlan-id*

Parameters

- **interface** *interface-id*—Port Identifier (Ethernet port or port channel).
- **vlan** *vlan-id*—VLAN Identifier.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays policies of all IPv6 First Hop Security attached to a VLAN specified by the *vlan-id* argument and displays all policies attached to a port and to VLAN specified by the *interface-id* and *vlan-id* arguments.

Examples

The following example displays the attached policy on gi1/0/1 and VLAN 100:

```
switchxxxxxx# show ipv6 first hop security attached policies interface gi1/0/1 vlan 100
Attached to VLAN 100
  RA Guard Policy: policy1
  Neighbor Bind Policy: policy2
Attached to port gi1/0/1 and VLAN 100
  IPv6 First Hop Security Policy: FHSpolicy
  ND Inspection Policy: policy1
  RA Guard Policy: policy3
  Neighbor Bind Policy: policy3
  IPv6 Source Guard Policy: policy4
```

show ipv6 first hop security counters

To display information about the packets counted by the port counter, use the **show ipv6 first hop security counters** command in privileged EXEC mode.

Syntax

show ipv6 first hop security counters interface *interface-id*

Parameters

- **interface** *interface-id*—Displays counters for specified Ethernet port or port channel.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays packets handled by the switch that are being counted in port counters. The switch counts packets captured per port and records whether the packet was received, bridged, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples displays information about packets counted on port gi1/0/1:

```
switchxxxxxx# show ipv6 first hop security counters interface gi1/0/1
Received messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[63] RS[0] NA[13] NS[0] REDIR[0]
  DHCPv6     ADV[0] REP[20] REC[0] REL-REP[0] LEAS-REP[10] RLS[0] DEC[0]
Dropped messages on gi1/0/1:
  Protocol   Protocol message
  NDP        RA[2] RS[0] NA[0] NS[0] REDIR[0]
  DHCPv6     ADV[1] REP[2] REC[0] REL-REP[1] LEAS-REP[0] RLS[0] DEC[0]
Dropped reasons on gi1/0/1:
  Feature         Number Reason
  DHCP Guard           2  Server message on client port
  DHCP Guard           1  Unauthorized assigned address
  DHCP Guard           1  Unauthorized server source address
  DHCP Guard           0  Unauthorized server preference
  RA guard             1  Router message on host port
  RA guard             1  Unauthorized source address
  RA guard             0  Unauthorized advertise prefix
  RA guard             0  Unauthorized router preference
  RA guard             0  Unauthorized other config flag
  RA guard             0  Unauthorized managed config flag
  RA guard             0  Unauthorized cur hop limit
  ND Inspection        0  Invalid source MAC
  ND Inspection        0  Unsecure message
  ND Inspection        0  Unauthorized sec level
  Source guard         0  NoBinding
  NB Integrity         0  Illegal ICMPv6 message
  NB Integrity         0  Illegal DHCPv6 message
```

show ipv6 first hop security error counters

To display global error counters, use the **show ipv6 first hop security error counters** command in privileged EXEC mode.

Syntax

show ipv6 first hop security error counters

Command Mode

Privileged EXEC mode

User Guidelines

This command displays global error counters.

Example 1—The following examples displays global error counters:

```
switchxxxxxx# show ipv6 first hop security error counters
Neighbor Binding Table Overflow counter: 0
Neighbor Prefix Table Overflow counter: 0
TCAM Overflow counter: 0
```

show ipv6 first hop security policy

To display IPv6 First Hop Security policies on all ports configured with the IPv6 First Hop Security feature, use the **show ipv6 first hop security policy** command in privileged EXEC mode.

Syntax

show ipv6 first hop security policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the IPv6 First Hop policy with the given name.
- **active**—Displays the attached Ipv6 First Hop Security policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the options configured for the policy on all ports configured with the IPv6 First Hop feature.

Example 1—The following example displays the Policy Configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 first hop security policy policy1
IPv6D First Hop Security Policy: policy1
  logging packet drop: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 first hop security policy active
Attached to VLAN:
  Policy Name   VLANs
  policy2       200-300
  vlan-default  1-199,301-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-2	1-100
	port-default	gi1/0/1-2	101-4094
		gi1/0/3-4	1-1094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 first hop security policy
policy1
policy2
```

show ipv6 nd inspection

To display ND Inspection global configuration, use the **show ipv6 nd inspection** command in Privilege EXEC configuration mode.

Syntax

show ipv6 nd inspection

Command Mode

Privileged EXEC mode

User Guidelines

This command displays ND Inspection global configuration.

Example

The following example gives an example of the **show ipv6 nd snooping** command output:

```
switchxxxxxx# show ipv6 nd snooping
IPv6 ND Inspection is enabled on VLANs:1-4,6,7,100-120
unsecure drop: enabled
sec-level minimum value: 2
source mac validation: disabled
```

show ipv6 nd inspection policy

To display an IPv6 ND Inspection policy on all ports configured with the ND Inspection feature, use the **show ipv6 nd inspection policy** command in privileged EXEC mode.

Syntax

show ipv6 nd inspection policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the ND Inspection policy with the given name.
- **active**—Displays the attached ND Inspection policies.

Command Mode

Privileged EXEC mode

Examples

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 nd inspection policy policy1
ND Inspection Policy: policy1
  device-role: router
  drop-unsecure: enabled
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 nd inspection policy active
Attached to VLANs:
  Policy Name   VLANs
  vlan-default  1-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-2	1-100
	port-default	gi1/0/1-2	101-4094
		gi1/0/3-4	1-1094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 nd inspection policy
policy1
policy2
```

show ipv6 nd raguard

To display RA Guard global configuration, use the **show ipv6 nd raguard** command in Privilege EXEC configuration mode.

Syntax

show ipv6 nd raguard

Command Mode

Privileged EXEC mode

Example

The following example gives an example of the **show ipv6 nd raguard** command output:

```
switchxxxxxx# show ipv6 nd raguard
IPv6 RA Guard is enabled on VLANs:1-4,6,7,100-120
"Managed address configuration" flag (M-flag:) off
"Other configuration" flag (O-flag): disabled
Hop Limit:
  minimum: 10
  maximum: 100
Default Router Preference:
  minimum: 1
  maximum: 1
```

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all ports configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

Syntax

show ipv6 nd raguard policy [*policy-name* | **active**]

Parameters

- ***policy-name***—Displays the RA guard policy with the given name.
- **active**—Displays the attached user defined RA guard policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the options configured for the policy on all ports configured with the RA guard feature.

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 nd raguard policy raguard1
RA Guard Policy: policy1
  device-role: router
  router address prefix list name: list1
  prefixes prefix list name: list2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 nd raguard policy active
Attached to VLANs:
  Policy Name   VLANs
```

```
  vlan-default  1-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	port-default	gi1/0/1-4	1-4094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 nd raguard policy
policy1
policy2
```

show ipv6 neighbor binding

To display Neighbor Binding global configuration, use the **show ipv6 neighbor binding** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding

Command Mode

Privileged EXEC mode

User Guidelines

This displays Neighbor Binding global configuration.

Example

The following example gives an example of the **show ipv6 neighbor binding** command output:

```
switchxxxxxx# show ipv6 neighbor binding
Neighbor Binding Integrity is enabled on VLANs:1-4,6-7,100-120
Binding logging: disabled
Binding lifetime: 56 minutes
Address Configuration method: dhcp
Binding address prefix validation: disabled
Maximum entries
 VLAN: unlimited
 Port: 1
 MAC: 1
```

show ipv6 neighbor binding policy

To display Neighbor Binding policies, use the **show ipv6 neighbor binding policy** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding policy [*policy-name* | active]

Parameters

- ***policy-name***—Neighbor Binding policy name.
- **active**—Displays the attached Neighbor Binding policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command either displays all policies or a specific one.

Examples

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 neighbor binding policy policy1
Neighbor Binding Policy: policy1
  address configuration method: dhcp
  binding address prefix validation: disabled
  device-role: perimiter
  binding logging: disabled
  max-entries
   VLAN: unlimited
   Port: 10
   MAC: 2
  Attached to VLANs: 1-100,111-4094
  Attached to ports:
```

	Ports	VLANs
	gi1/0/1-2	1-58,68-4094
	gi1/0/3-4	1-4094
	Po1-4	1-4094

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 neighbor binding policy active
Attached to VLAN:
  Policy Name     VLANs
  policy2         200-300
  vlan-default    1-199,301-4094
Attached to ports:
```

	Policy Name	Ports	VLANs
	policy1	gi1/0/1-4	1-100
	port-default	gi1/0/1-4	101-4094

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 neighbor binding policy
policy1
policy2
```

show ipv6 neighbor binding prefix table

To display contents of the Neighbor Prefix table, use the **show ipv6 neighbor binding prefix table** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding prefix table [**vlan** *vlan-id*]

Parameters

- **vlan** *vlan-id*—Displays the prefixes that match the specified VLAN.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays the Neighbor Prefix table. The display output can be limited to the specified VLAN. If no VLAN is configured, all prefixes are displayed.

Example

The following example displays the learned prefixes:

```
switchxxxxxx# show ipv6 neighbor binding prefix table
Flags: A - the prefix can be used for autoconfig (stateless configuration)
Neighbor Prefix Table has 4 entries
VLAN  Prefix         Type    Flags   Remaining Lifetime
   7  2004:1::/64   static    A
   7  2006:1::/64   dynamic              1230
   7  2008:1::/64   static
1027  2002:1::/64   dynamic   A            230
```

show ipv6 neighbor binding table

To display contents of the Binding table, use the **show ipv6 neighbor binding table** command in Privilege EXEC configuration mode.

Syntax

show ipv6 neighbor binding table [**vlan** *vlan-id*] [**interface** *interface-id*] [**ipv6** *ipv6-address*] [**mac** *mac-address*]

Parameters

- **vlan** *vlan-id*—Displays the Binding table entries that match the specified VLAN.
- **interface** *interface-id*—Displays the Binding table entries that match the specified port (Ethernet port or port channel).

- **ipv6** *ipv6-address*—Displays the Binding table entries that match the specified IPv6 address.
- **mac** *mac-address*—Displays the Binding table entries that match the specified MAC address.

Command Mode

Privileged EXEC mode

User Guidelines

This displays the contents of the Binding table. The display output can be specified by the specified VLAN, port, IPv6 address, or MAC address. If no keywords or arguments are entered, all Binding table contents are displayed.

Any keyword and argument combinations are allowed.

Example

The following example displays the contents of the Binding table:

```
switchxxxxxx# show ipv6 neighbor binding table
Binding Table has 4 entries
```

VLAN	IPv6 address	Inter	MAC address	Origin	State	Expir	TCAM
-----	----------	-------	--------------	------	-----	Time	Ovrfl
100	2001:300::1	gi1/0/1	AABB.CC01.F500	NDP	VALID	------	-----
100	2001:600::1	gi1/0/1	AABB.CC01.F510	NDP	TENT	559	*
100	2001:100::2	gi1/0/2	AABB.CC01.F160	NDP	VALID	96	
200	2001:200::3	gi1/0/2			VALID	79	

```
Field Descriptions:
```

- **VLAN**—VLAN the host belongs to.
- **IPv6 address**—IPv6 address of the host.
- **Inter**—port the host is connected on.
- **MAC address**—MAC address of the host.
- **Origin**—Protocol that has added the IPv6 address:
- **Static**—The static IPv6 address manually defined by the i**pv6 neighbor binding static** command.
- **NDP**—The IPv6 address learnt from the NDP protocol messages.
- **DHCP**—The IPv6 address learnt from the DHCPv6 protocol messages.
- **State**—Entry's state:
- **TENT**—The new host IPv6 address is under validation. Since its lifetime is less than 1sec its expiration time is not displayed.
- **VALID**—The host IPv6 address was bound.
- **Expir. Time**—Left time in seconds until the entry will be removed, if it is not confirmed.

- **TCAM Ovrflw**—Entries marked by '*' have not been added to TCAM because TCAM overflow.

show ipv6 source guard

To display IPv6 Source Guard global configuration, use the **show ipv6 source guard** command in Privilege EXEC configuration mode.

Syntax

show ipv6 source guard

Parameters

N/A

Command Mode

Privileged EXEC mode

User Guidelines

This displays IPv6 Source Guard global configuration.

Example

The following example gives an example of the **show ipv6 source guard** command output:

```
switchxxxxxx# show ipv6 source guard
IPv6 Source Guard is enabled on VLANs:1-4,6,7,100-120
```

show ipv6 source guard policy

To display IPv6 Source Guard policies, use the **show ipv6 source guard policy** command in Privilege EXEC configuration mode.

Syntax

show ipv6 source guard policy [*policy-name* | active]

Parameters

- ***policy-name***—IPv6 Source Guard policy name.
- **active**—Displays the attached IPv6 Source Guard policies.

Command Mode

Privileged EXEC mode

User Guidelines

This command displays all configured IPv6 Source Guard policies, the given one or all attached IPv6 Source Guard policies.

Example 1—The following example displays the policy configuration for a policy named policy1:

```
switchxxxxxx# show ipv6 source guard policy policy1
Neighbor Binding Policy: policy1
  trusted port: disabled
  Attached to ports:
   Ports
   gi1/0/1-2
   gi1/0/4
   Po1-4
```

Example 2—The following example displays the attached policies:

```
switchxxxxxx# show ipv6 source guard policy active
Attached to VLAN:
Attached to ports:
```

	Policy Name	Ports
	policy1	gi1/0/1-2
	port-default	gi1/0/1-2
		gi1/0/3

Example 3—The following example displays the user defined policies:

```
switchxxxxxx# show ipv6 source guard policy
policy1
policy2
```

trusted-port (IPv6 Source Guard)

To configure a port as trusted port within an IPv6 Source Guard policy, use the **trusted-port** command in IPv6 Source Guard Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

trusted-port

no trusted-port

Default Configuration

not trusted.

Command Mode

IPv6 Source Guard Policy Configuration mode

User Guidelines

IPv6 data messages bridged from trusted ports are not validated by IPv6 Source Guard.

Example

The following example defines a policy that defines a port as trusted:

```
switchxxxxxx(config)# ipv6 ipv6 source guard policy policy1
switchxxxxxx(config-ipv6-srcguard)# trusted-port
switchxxxxxx(config-ipv6-srcguard)# exit
```

validate source-mac

To enable checking the MAC addresses against the link-layer address within an IPv6 ND Inspection policy, use the **validate source-mac** command in ND Inspection Policy Configuration mode. To return to the default, use the **no** form of this command.

Syntax

validate source-mac [enable | disable]

no validate source-mac

Parameters

- **enable**—Enables validation of the MAC address against the link-layer address. If no keyword is configured, this keyword is applied by default.
- **disable**—Disables validation of MAC address against the link-layer address.

Default Configuration

Policy attached to port or port channel: the value configured in the policy attached to the VLAN.

Policy attached to VLAN: global configuration.

Command Mode

ND inspection Policy Configuration mode

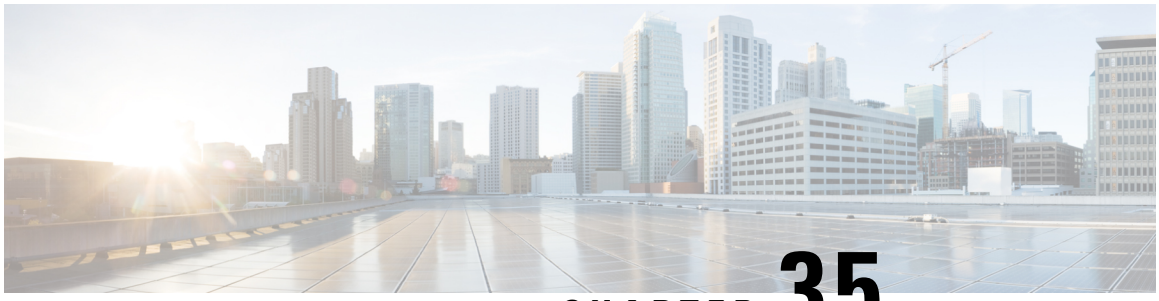
User Guidelines

If this command is part of a policy attached to a VLAN, it is applied to all the ports in the VLAN. If it is defined in a policy attached to a port in the VLAN, this value overrides the value in the policy attached to the VLAN.

Example

The following example enables the router to drop an NDP message whose link-layer address does not match the MAC address:

```
switchxxxxxx(config)# ipv6 nd inspection policy policy1
switchxxxxxx(config-nd-inspection)# validate source-mac
switchxxxxxx(config-nd-inspection)# exit
```



CHAPTER 35

IPv6 IPM Router Commands

This chapter contains the following sections:

- ipv6 multicast hop-threshold, on page 607
- ipv6 multicast-routing, on page 608
- show ipv6 mroute, on page 609
- show ipv6 multicast, on page 610

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

ipv6 multicast hop-threshold *hop-value*

no ipv6 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 mode

User Guidelines

Multicast packets with a hop value less than the threshold will not be forwarded on the interface.

The default value of 0 means all Multicast packets are forwarded on the interface.

A value of 256 means that no Multicast packets are forwarded on 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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 multicast hop-threshold 200
switchxxxxxx(config-if)# exit
```

ipv6 multicast-routing

To enable IPv6 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 mld-proxy

no ipv6 multicast-routing

Parameters

- **mld-proxy**—Enable Multicast routing using MLD Proxy.

Default Configuration

Multicast routing is not enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the **ipv6 multicast-routing** command with parameter to specify the needed IPv6 Multicast Routing Protocol.

To forward IPv6 Multicast packets on an interface, 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:

```
switchxxxxxx(config)# ipv6 multicast-routing mld-proxy
```

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***—Destination Multicast IPv6 address.
- ***source-address***—Source IPv6 address.
- **summary**—Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.

Command Mode

User EXEC mode

Privileged EXEC mode

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]).

Examples

Description of Significant fields in the examples below

Timers:Uptime/Expires—"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IPv6 Multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 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.

Incoming interface: —Expected interface for a Multicast packet from the source. If the packet is not received on this interface, it is discarded.

Outgoing Interface List (OIF):—Interfaces through which packets will be forwarded.

Example 1. The following is sample output from the **show ipv6 mroute** command with the summary keyword:

```
switchxxxxxx# show ip mroute summary
Timers: Uptime/Expires
IPv6 Multicast Routing Table
(2001:0DB8:999::99, FF07::5), 00:04:55/00:02:36, OIF count:1
(2001:0DB8:999::99, FF07::1), 00:02:46/00:00:12, OIF count:1
```

Example 2. The following is sample output from the **show ipv6 mroute** command:

```
switchxxxxxx# show ip mroute
Timers: Uptime/Expires
IPv6 Multicast Routing Table
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6
  Incoming interface: vlan5
  Outgoing interface list:
    vlan40, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23
  Incoming interface: vlan5
  Outgoing interface list:
    vlan40, 00:02:06/00:03:27
```

show ipv6 multicast

To display general information about IPv6 Multicast configuration, 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 IPv6 Multicast.
- ***interface-id***—Interface identifier for which to display IPv6 Multicast information.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use the **show ipv6 multicas**t command without the **interface** keyword to display general information about the state of IPv6 Multicast on the router.

Use the **show ipv6 multicast** command with the **interface** keyword to display the IPv6 Multicast information about the specified interface.

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:

```
switchxxxxxx# show ipv6 multicast
IPv6 Unicast Forwarding: enabled
IPv6 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:

```
switchxxxxxx# 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:

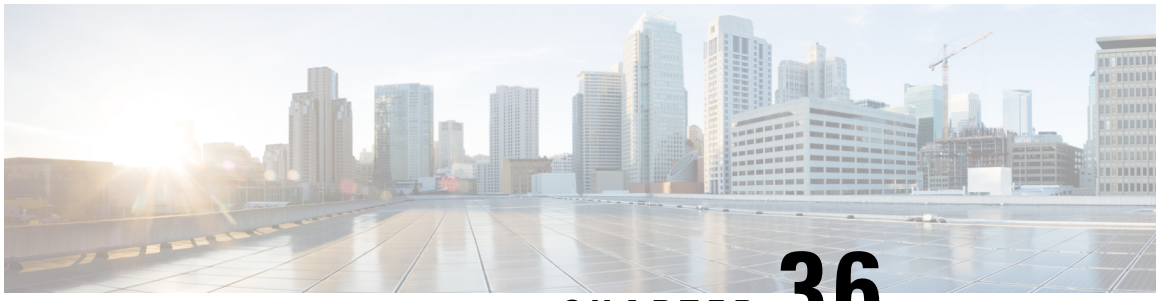
```
switchxxxxxx# show ipv6 multicast interface vlan 200
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
vlan 200
 IPv6 Status: enabled
 hop-threshold: 0
 MLD Protocol: MLDv2
 MLD Proxy: Upstream
```

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:

```
switchxxxxxx# show ipv6 multicast interface vlan 100
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: PIM
vlan 200
 IPv6 Status: enabled
 hop-threshold: 0
 MLD Protocol: MLDv2
 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:

```
switchxxxxxx# show ipv6 multicast interface vlan 100
IPv6 Unicast Forwarding: enabled
IPv6 Multicast Protocol: MLD Proxy
vlan 200
 IPv6 Status: enabled
 hop-threshold: 100
 MLD Protocol: MLDv2
 MLD Proxy: disabled
```



CHAPTER 36

IPv6 Prefix List Commands

This chapter contains the following sections:

- clear ipv6 prefix-list, on page 613
- ipv6 prefix-list, on page 614
- show ipv6 prefix-list, on page 617

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 mode

User Guidelines

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:

```
switchxxxxxx# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

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. This 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*—Text that can be up to 80 characters in length.
- **ge** *ge-value*—Specifies a prefix length greater than or equal to the /*prefix-length* argument. 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 /*prefix-length* argument. 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 mode

User Guidelines

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.

This command without the **seq** keyword removes the prefix list.

The **no** version of this 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.

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 the following conditions must 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 0 up to the value of the *le-length* argument, and including, this value.

  The value of the optional **ge** keyword specifies the range of allowed prefix lengths from the value of the *ge-length* argument 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 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 1. The following example denies all routes with a prefix of ::/0:

```
switchxxxxxx(config)# ipv6 prefix-list abc deny ::/0
```

Example 2. The following example permits the prefix 2002::/16:

```
switchxxxxxx(config)# 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:

```
switchxxxxxx(config)# 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:

```
switchxxxxxx(config)# 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:

```
switchxxxxxx(config)# 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:

```
switchxxxxxx(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

Example 7. The following example denies all routes with a prefix of 2002::/128:

```
switchxxxxxx(config)# ipv6 prefix-list abc deny 2002::/128
```

Example 8. The following example permits all routes with a prefix of ::/0:

```
switchxxxxxx(config)# ipv6 prefix-list abc permit ::/0
```

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** | f**irst-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 mode

Privileged EXEC mode

User Guidelines

If the **detail** and **summary** keywords are omitted, the **detail** option is applied.

If the **longer** and **first-match** keywords are omitted, all entries of the specified prefix list that matches the given network/length are displayed.

Example 1. The following example shows the output of this command with the **detail** keyword:

```
switchxxxxxx# 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)
```

Field Descriptions

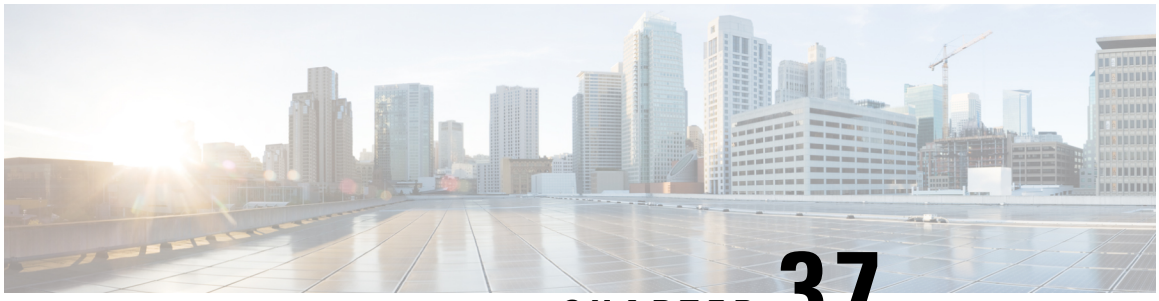
- **count**—Number of entries in the list.
- **range entries**—Number of entries with matching range.
- **seq**—Entry number in the list.
- **permit, deny**—Granting status.
- **description**—Comment.
- **hit count**—Number of matches for the prefix entry.

Example 2. The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword:

```
switchxxxxxx# show ipv6 prefix-list summary
ipv6 prefix-list 6to4:
  count: 1, range entries: 0
ipv6 prefix-list aggregate:
  count: 2, range entries: 2
```

Example 3. The following example shows the output of the **show ipv6 prefix-list** command with the **seq** keyword:

```
switchxxxxxx# show ipv6 prefix-list bgp-in seq 15
  seq 15 deny ::/1 (hit count: 0)
```



CHAPTER 37

iSCI QoS Commands

This chapter contains the following sections:

- iscsi enable, on page 619
- iscsi flow, on page 620
- iscsi qos, on page 621
- show iscsi, on page 622

iscsi enable

To enable applying the quality of service profile to Internet Small Computer System Interface (iSCSI) flows, use the **iscsi enable** command in Global Configuration mode. To restore the default configuration, use the **no** form of the command.

Syntax

iscsi enable

no iscsi enable

Parameters

This command has no arguments or keywords

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

Use the **iscsi enable** command to enable the iSCSI QoS.

If an ACL is bounded on an interface and a frame matches both to the iSCLI and the ACL rules then only the iSCSI rules are applied to this frame.

Example

The following example enables iSCSI QoS globally:

```
switchxxxxxx(config)# iscsi enable
```

iscsi flow

To define an iSCSI flow, use the **iscsi flow** command in Global Configuration mode. To remove the iSCSI flow, use the **no** form of the command.

Syntax

iscsi flow default | {*tcp-port* [*ip-address*]}

no iscsi flow [default | {*tcp-port* [*ip-address*]}]

Parameters

- **default**—Restores the default IPv4 flows.
- ***tcp-port***—Specifies the TCP port number on which iSCSI targets listen to requests. (Range: 1–65535)
- ***ip-address***—Specifies the IPv4 address on which iSCSI targets listen to requests.

Default Configuration

Two iSCSI IPv4 flows with well-known TCP ports 3260 and 860.

Command Mode

Global Configuration mode

User Guidelines

Each **iscsi flow** command defines an iSCSI flow including the following two sub-flows:

- From initiator to target sub-flow—The sub-flow is classified by the Destination TCP port defined by the *tcp-port* argument and by the configured Destination IP address, if the *ip-address* argument is configured.
- From target to initiator sub-flow—The sub-flow is classified by the Source TCP port defined by the *tcp-port* argument and by the configured Source IP address, if the *ip-address* argument is configured.

Up to 8 iSCSI flows are supported.

Use the **iscsi flow default** command, to restore the iSCSI default configuration.

For the same TCP port you can use either the **iscsi flow** *tcp-port* command or a few **iscsi flow** *tcp-port ip-address* commands with different IP addresses.

Use the **no iscsi flow** *tcp-port ip-address* command, to delete the iSCSI flows defined by the **iscsi target port** *tcp-port ip-address* command.

Use the **no iscsi flow** *tcp-port* command, to delete the iSCSI flows defined by the **iscsi flow** *tcp-port* command.

To delete a default iSCSI flow, use the **no iscsi flow** *tcp-port* command.

To delete all default iSCSI flows, use the **no iscsi flow default** command.

To delete all iSCSI flows (including the default ones), use the **no iscsi flow** command.

Example

The following example defines four pair of iSCSI flows:

```
switchxxxxxx(config)# no iscsi flow default
switchxxxxxx(config)# iscsi flow 1200
switchxxxxxx(config)# iscsi flow 1201 1.1.1.1
switchxxxxxx(config)# iscsi flow 1201 1.1.1.10
switchxxxxxx(config)# iscsi flow 1201 101.12.21.410
```

iscsi qos

To define the quality of service profile applying to iSCSI flows, use the **iscsi qos** command in Global Configuration mode. To restore the default configuration, use the **no** form of the command.

Syntax

iscsi qos {[**vpt** *vpt*] [**dscp** *dscp*] [**queue** *queue*]}

no iscsi qos

Parameters

- **vpt** *vpt*—Specifies a value of the VLAN Priority Tag (VPT) that iSCSI tagged frames are assigned (Range: 0–7).
- **dscp** *dscp*—Specifies the Differentiated Services Code Point (DSCP) that iSCSI frames are assigned. (Range: 0–63).
- **queue** *queue*—Specify the outgoing queue that iSCSI frames are sent (Range: 1–8).

Default Configuration

- VPT is not changed.
- DSCP is not changed.
- Queue—7

Command Mode

Global Configuration mode

User Guidelines

Use the **iscsi qos** command, to change the default quality of service profile applying to iSCSI flows.

Note. At least one parameter is mandatory

Example

The following example configures the default quality of service profile applying to iSCSI flows:

```
switchxxxxxx(config)# iscsi qos vpt 6 queue 8
```

show iscsi

To display the iSCSI configuration, use the **show iscsi** command in User EXEC mode.

Syntax

show iscsi

Parameters

This command has no arguments or keywords

Default Configuration

This command has no default settings.

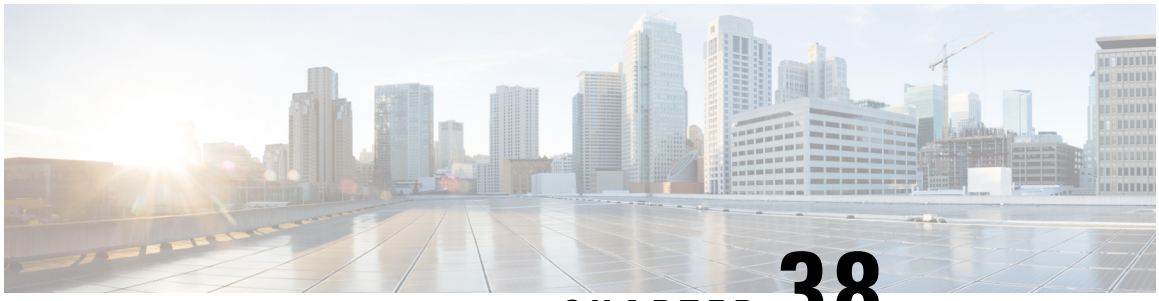
Command Mode

User EXEC mode

Example

This example shows how to display the iSCSI configuration:

```
switchxxxxxx> show iscsi
iSCSI is enabled
iSCSI vpt is not changed
iSCSI DSCP is 18
iSCSI Queue is 7 (default)
iSCSI Flows:
  TCP         Target IP
  Port        Address
---------  ---------------
   860     0.0.0.0            default
  3260     0.0.0.0            default
  9876     0.0.0.0
  20002    192.111.220.110
  20002    192.1.3.230
  25555    0.0.0.0
```



CHAPTER 38

Line Commands

This chapter contains the following sections:

- exec-timeout, on page 623
- line, on page 624
- show line, on page 624
- speed, on page 625

exec-timeout

To set the session idle time interval, during which the system waits for user input before automatic logoff, use the **exec-timeout** Line Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

exec-timeout *minutes* [*seconds*]

no exec-timeout

Parameters

- **minutes**—Specifies the number of minutes. (Range: 0-65535)
- **seconds**—(Optional) 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
```

line

To identify a specific line for configuration and enter the Line Configuration command mode, use the **line** Global Configuration mode command.

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)#
```

show line

To display line parameters, use the **show line** Privileged EXEC mode command.

Syntax

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

Parameters

- **console**—(Optional) Displays the console configuration.
- **telnet**—(Optional) Displays the Telnet configuration.
- **ssh**—(Optional) Displays the SSH configuration.

Default Configuration

If the line is not specified, all line configuration parameters are displayed.

Command Mode

Privileged 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
```

speed

To set the line baud rate, use the **speed** command in Line Configuration mode.

To restore the default configuration, use the **no** form of this command.

Syntax

speed *bps*

no speed

Parameters

bps—Specifies the baud rate in bits per second (bps). Possible values are 9600, 19200, 38400, 57600, and 115200.

Default Configuration

The default speed is 115200 bps.

Command Mode

Line Configuration Mode

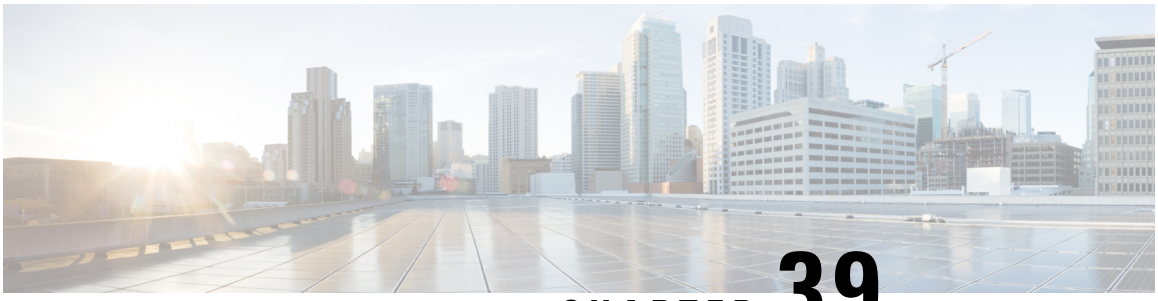
User Guidelines

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
```



CHAPTER 39

LACP Commands

This chapter contains the following sections:

- lacp port-priority, on page 627
- lacp system-priority, on page 628
- lacp timeout, on page 628
- show lacp, on page 629
- show lacp port-channel, on page 631

lacp port-priority

To set the physical port priority, use the **lacp port-priority** Interface (Ethernet) Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

value—Specifies the port priority. (Range: 1–65535)

Default Configuration

The default port priority is 1.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example sets the priority of gi1/0/6.

```
switchxxxxxx(config)#  interface gi1/0/6
switchxxxxxx(config-if)#  lacp port-priority 247
```

lacp system-priority

To set the system priority, use the **lacp system-priority** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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
```

lacp timeout

To assign an administrative LACP timeout to an interface, use the **lacp timeout** Interface (Ethernet) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet) Configuration mode

Example

The following example assigns a long administrative LACP timeout to gi1/0/6.

```
switchxxxxxx(config)#  interface gi1/0/6
switchxxxxxx(config-if)#  lacp timeout long
```

show lacp

To display LACP information for all Ethernet ports or for a specific Ethernet port, use the **show lacp** Privileged EXEC mode command.

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**—(Optional) Displays parameters only.
- **statistics**—(Optional) Displays statistics only.
- **protocol-state**—(Optional) Displays protocol state only.

Command Mode

Privileged EXEC mode

Example

The following example displays LACP information for gi1/0/1.

switchxxxxxx# **show lacp ethernet gi1/0/1**	
Port gi1/0/1 LACP parameters:	
	Actor

		system priority: system mac addr: port Admin key: port Oper key: port Oper number: port Admin priority: port Oper priority: port Admin timeout: port Oper timeout: LACP Activity: Aggregation: synchronization: collecting: distributing: expired:	1 00:00:12:34:56:78 30 30 21 1 1 LONG LONG ACTIVE AGGREGATABLE FALSE FALSE FALSE FALSE
	Partner		
		system priority: system mac addr: port Admin key: port Oper key: port Oper number: port Admin priority: port Oper priority: port Admin timeout: port Oper timeout: LACP Activity: Aggregation: synchronization: collecting: distributing: expired:	0 00:00:00:00:00:00 0 0 0 0 0 LONG LONG PASSIVE AGGREGATABLE FALSE FALSE FALSE FALSE
Port gi1/0/1 LACP Statistics: LACP PDUs sent: LACP PDUs received:			2 2
Port gi1/0/1 LACP Protocol State:			
	LACP State Machines:		
		Receive FSM: Mux FSM:	Port Disabled State Detached State
	Control Variables:		
		BEGIN: LACP_Enabled: Ready_N: Selected: Port_moved: NNT: Port_enabled:	FALSE TRUE FALSE UNSELECTED FALSE FALSE FALSE
	Timer counters:		
		periodic tx timer: current while timer: wait while timer:	0 0 0

show lacp port-channel

To display LACP information for a port-channel, use the **show lacp port-channel** Privileged EXEC mode command.

Syntax

show lacp port-channel *[port_channel_number]*

Parameters

port_channel_number—(Optional) Specifies the port-channel number.

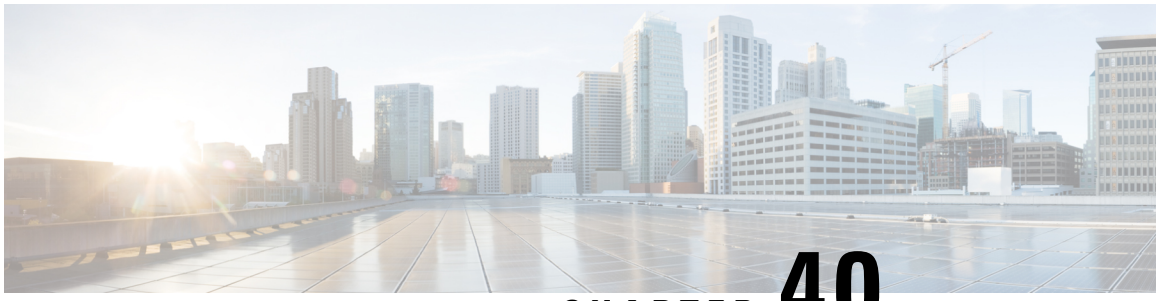
Command Mode

Privileged 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 Priority: MAC Address: Admin Key: Oper Key:	1 000285:0E1C00 29 29
	Partner		
		System Priority: MAC Address: Oper Key:	0 00:00:00:00:00:00 14



CHAPTER 40

LLDP Commands

This chapter contains the following sections:

- clear lldp statistics, on page 634
- clear lldp table , on page 634
- lldp chassis-id, on page 635
- lldp hold-multiplier, on page 636
- lldp lldpdu , on page 636
- lldp management-address, on page 637
- lldp med, on page 638
- lldp med notifications topology-change, on page 639
- lldp med fast-start repeat-count, on page 639
- lldp med location, on page 640
- lldp med network-policy (global), on page 641
- lldp med network-policy (interface), on page 642
- lldp med network-policy voice auto, on page 643
- lldp notifications, on page 644
- lldp notifications interval, on page 644
- lldp optional-tlv, on page 645
- lldp optional-tlv 802.1, on page 646
- lldp run , on page 647
- lldp receive , on page 647
- lldp reinit , on page 648
- lldp timer, on page 648
- lldp transmit , on page 649
- lldp tx-delay, on page 650
- show lldp configuration, on page 650
- show lldp local, on page 652
- show lldp local tlvs-overloading, on page 654
- show lldp med configuration, on page 654
- show lldp neighbors, on page 655
- show lldp statistics, on page 659

clear lldp statistics

Use the **clear lldp statistics** command in Privileged EXEC mode to clear LLDP statistics on device.

Syntax

clear lldp statistics [**global** | *interface-id*]

Parameters

- **global**—(Optional) clears only the global LLDP table statistics.
- ***interface-id***—(Optional) Clears the counters only for specified port ID

Default Configuration

Clears all LLDP statistics - global statistics and all interface counters.

Command Mode

Privileged EXEC mode

User Guidelines

Use the command **clear lldp statistics** without parameters to clear all LLDP statistics on device. This clears both global LLDP table statistics and all the interface counters.

Use the **clear lldp statistics global** to clear only the global LLDP table statistics.

Use the **clear lldp statistics** *interface-id* command to clear the counters of the given interface.

Examples

The following example clears lldp counter from interface gi1/0/1

```
switchxxxxxx#  clear lldp statistics gi1/0/1
```

clear lldp table

To clear the neighbors table for all ports or for a specific port, use the **clear lldp table** command in Privileged EXEC mode.

Syntax

clear lldp table *[interface-id]*

Parameters

interface-id—(Optional) 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

```
switchxxxxxx#  clear lldp table gi1/0/1
```

lldp chassis-id

To configure the source of the chassis ID of the port, use the **lldp chassis-id** Global Configuration mode command. To restore the chassis ID source to default, use the **no** form of this command.

Syntax

lldp chassis-id *{***mac-address** | **host-name***}*

no lldp chassis-id

Parameters

- **mac-address**—Specifies the chassis ID to use the device MAC address.
- **host-name**—Specifies the chassis ID to use the device configured host name.

Default Configuration

MAC address.

Command Mode

Global Configuration mode

User Guidelines

The host name should be configured to be a unique value.

If the chassis ID configured to be used in LLDP packets is empty, LLDP uses the default chassis ID (specified above).

Example

The following example configures the chassis ID to be the MAC address.

```
switchxxxxxx(config)#  lldp chassis-id mac-address
```

lldp hold-multiplier

To specify how long the receiving device holds a LLDP packet before discarding it, use the **lldp hold-multiplier** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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.

```
switchxxxxxx(config)#  lldp timer 30
switchxxxxxx(config)#  lldp hold-multiplier 3
```

lldp lldpdu

To define LLDP packet handling when LLDP is globally disabled, use the **lldp lldpdu** Global Configuration mode command. 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** and vice versa.

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.

```
switchxxxxxx(config)#  lldp lldpdu flooding
```

lldp management-address

To specify the management address advertised by an interface, use the **lldp management-address** Interface (Ethernet) Configuration mode command. To stop advertising management address information, use the **no** form of this command.

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 (Ethernet) Configuration mode

User Guidelines

Each port can advertise one IP address.

Example

The following example sets the LLDP management address advertisement mode to **automatic** on gi1/0/2.

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp management-address automatic
```

lldp med

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

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, and POE-PSE, Inventory. The Capabilities TLV is always included if LLDP-MED is enabled.
- **disable**—Disable LLDP MED on the port

Default Configuration

Enabled with network-policy TLV

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example enables LLDP MED with the **location** TLV on gi1/0/3.

```
switchxxxxxx(config)#  interface gi1/0/3
switchxxxxxx(config-if)#  lldp med enable location
```

lldp med notifications topology-change

To enable sending LLDP MED topology change notifications on a port, use the **lldp med notifications topology-change** Interface (Ethernet) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet) Configuration mode

Example

The following example enables sending LLDP MED topology change notifications on gi1/0/2.

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp med notifications topology-change enable
```

lldp med fast-start repeat-count

When a port comes up, LLDP can send packets more quickly than usual using its fast-start mechanism.

To configure the number of packets that is sent during the activation of the fast start mechanism, use the **lldp med fast-start repeat-count** Global Configuration mode command. To return to default, use the **no** form of this command.

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

```
switchxxxxxx(config#  lldp med fast-start repeat-count 4
```

lldp med location

To configure the location information for the LLDP Media Endpoint Discovery (MED) for a port, use the **lldp med location** Interface (Ethernet) Configuration mode command. To delete location information for a port, use the **no** form of this command.

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 (Ethernet) Configuration mode

Example

The following example configures the LLDP MED location information on gi1/0/2 as a civic address.

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp med location civic-address 616263646566
```

lldp med network-policy (global)

To define a LLDP MED network policy, use the **lldp med network-policy** Global Configuration mode command. For voice applications, it is simpler to use lldp med network-policy voice auto, on page 643.

The **lldp med network-policy** command creates the network policy, which is attached to a port by lldp med network-policy (interface), on page 642.

The network policy defines how LLDP packets are constructed.

To remove LLDP MED network policy, use the **no** form of this command.

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*—(Optional) VLAN identifier for the application.

- **vlan-type**—(Optional) Specifies if the application is using a tagged or an untagged VLAN.
- **up** *priority*—(Optional) User Priority (Layer 2 priority) to be used for the specified application.
- **dscp** *value*—(Optional) 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-signal application and attaches it to port 1. LLDP packets sent on port 1 will contain the information defined in the network policy.

```
switchxxxxxx(config)#  lldp med network-policy 1 voice-signaling vlan 1 vlan-type untagged
 up 1 dscp 2
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp med network-policy add 1
```

lldp med network-policy (interface)

To attach or remove an LLDP MED network policy on a port, use the **lldp med network-policy** Interface (Ethernet) Configuration mode command. Network policies are created in lldp med network-policy (global), on page 641.

To remove all the LLDP MED network policies from the port, use the **no** form of this command.

Syntax

lldp med network-policy *{***add** | **remove***}* *number*

no lldp med network-policy *number*

Parameters

- **add/remove** *number*—Attaches/removes the specified network policy to the interface.
- **number**—Specifies the network policy sequential number. The range is 1-32

Default Configuration

No network policy is attached to the interface.

Command Mode

Interface (Ethernet) Configuration 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.

```
switchxxxxxx(config)#  lldp med network-policy 1 voice-signaling vlan 1 vlan-type untagged
 up 1 dscp 2
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp med network-policy add 1
```

lldp med network-policy voice auto

A network policy for voice LLDP packets can be created by using the lldp med network-policy (global), on page 641. The **lldp med network-policy voice au**to Global Configuration mode is simpler in that it uses the configuration of the Voice application to create the network policy instead of the user having to manually configure it.

This command generates an LLDP MED network policy for voice, if the voice VLAN operation mode is **auto voice VLAN**. The voice VLAN, 802.1p priority, and the DSCP of the voice VLAN are used in the policy.

To disable this mode, use the **no** form of this command.

The network policy is attached automatically to the voice VLAN.

Syntax

lldp med network-policy voice auto

no lldp med network-policy voice auto

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Global Configuration mode

User Guidelines

In Auto mode, the Voice VLAN feature determines on which interfaces to advertise the network policy TLV with application type **voice**, and controls the parameters of that TLV.

To enable the auto generation of a network policy based on the auto voice VLAN, there must be no manually pre-configured network policies for the voice application

In Auto mode, you cannot manually define a network policy for the voice application using the lldp med network-policy (global), on page 641 command.

Example

```
switchxxxxxx(config)#  lldp med network-policy voice auto
```

lldp notifications

To enable/disable sending LLDP notifications on an interface, use the **lldp notifications** Interface (Ethernet) Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 (Ethernet) Configuration mode

Example

The following example enables sending LLDP notifications on gi1/0/1.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp notifications enable
```

lldp notifications interval

To configure the maximum transmission rate of LLDP notifications, use the **lldp notifications interval** Global Configuration mode command. To return to the default, use the **no** form of this command.

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

```
switchxxxxxx(config)#  lldp notifications interval 10
```

lldp optional-tlv

To specify which optional TLVs are transmitted, use the **lldp optional-tlv** Interface (Ethernet) Configuration mode command. To restore the default configuration, use the **no** form of this 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, Power-via-MDI , 4-wirePower-via-MDI.

  none—(Optional) Clear all optional TLVs from the interface.

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

Default Configuration

The following TLV are transmitted:

- sys-name
- sys-cap

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example specifies that the port description TLV is transmitted on gi1/0/2.

```
switchxxxxxx(config)#  interface gi1/0/2
switchxxxxxx(config-if)#  lldp optional-tlv port-desc
```

lldp optional-tlv 802.1

To specify whether to transmit the 802.1 TLV, use the **lldp optional-tlv 802.1** Interface (Ethernet) Configuration mode command. To revert to the default setting, use the **no** form of this command.

Syntax

lldp optional-tlv 802.1 pvid *{**enable** | **disable**}* - The PVID is advertised or not advertised.

no lldp optional-tlv 802.1 pvid - The PVID advertise state is returned to default.

lldp optional-tlv 802.1 ppvid *add ppvid* - The Protocol Port VLAN ID (PPVID) is advertised. The PPVID is the PVID that is used depending on the packet's protocol.

lldp optional-tlv 802.1 ppvid *remove ppvid* - The PPVID is not advertised.

lldp optional-tlv 802.1 vlan *add vlan-id* - This *vlan-id* is advertised.

lldp optional-tlv 802.1 vlan *remove vlan-id* - This *vlan-id* is not advertised.

lldp optional-tlv 802.1 protocol *add {**stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp**}* - The protocols selected are advertised.

lldp optional-tlv 802.1 protocol *remove {***stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp***}* - The protocols selected are not advertised.

Parameters

- **lldp optional-tlv 802.1 pvid** *{**enable** | **disable**}*—Advertises or stop advertize the PVID of the port.
- **lldp optional-tlv 802.1 ppvid add/remove** *ppvid* —Adds/removes PPVID for advertising. (range: 0–4094). PPVID = 0 indicates that the port is not capable of supporting port and protocol VLANs and/or the port is not enabled with any protocol VLANs.
- **add/remove** *vlan-id*—Adds/removes VLAN for advertising (range: 1–4094).
- **add/remove** *{**stp** | **rstp** | **mstp** | **pause** | **802.1x** | **lacp** | **gvrp**}*—Add specifies to advertise the specified protocols; remove specifies not to advertise the specified protocol.

Default Configuration

The following 802.1 TLV is transmitted:

Command Mode

Interface (Ethernet) Configuration mode

Example

```
switchxxxxxx(config)#  lldp optional-tlv 802.1 protocol add stp
```

lldp run

To enable LLDP, use the **lldp run** Global Configuration mode command. To disable LLDP, use the **no** form of this command.

Syntax

lldp run

no lldp run

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)#  lldp run
```

lldp receive

To enable receiving LLDP on an interface, use the **lldp receive** Interface (Ethernet) Configuration mode command. To stop receiving LLDP on an Interface (Ethernet) Configuration mode interface, use the **no** form of this command.

Syntax

lldp receive

no lldp receive

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration 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

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp receive
```

lldp reinit

To specify the minimum time an LLDP port waits before reinitializing LLDP transmission, use the **lldp reinit** Global Configuration mode command. To revert to the default setting, use the **no** form of this command.

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

```
switchxxxxxx(config)#  lldp reinit 4
```

lldp timer

To specify how often the software sends LLDP updates, use the **lldp timer** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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.

```
switchxxxxxx(config)#  lldp timer 60
```

lldp transmit

To enable transmitting LLDP on an interface use the **lldp transmit** Interface (Ethernet) Configuration mode command. Use the **no** form of this command to stop transmitting LLDP on an interface,

Syntax

lldp transmit

no lldp transmit

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Interface (Ethernet) Configuration mode

switchxxxxxx(config-if)#

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

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  lldp transmit
```

lldp tx-delay

To set the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the **lldp tx-delay** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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 25% of the LLDP timer interval.

Example

The following example sets the LLDP transmission delay to 10 seconds.

```
switchxxxxxx(config)#  lldp tx-delay 10
```

show lldp configuration

To display the LLDP configuration for all ports or for a specific port, use the **show lldp configuration** Privileged EXEC mode command.

Syntax

show lldp configuration *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies the port ID.
- **detailed**—(Optional) 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 1 - Display LLDP configuration for all ports.

```
switchxxxxxx#  show lldp configuration
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Port      State  Optional TLVs      Address       Notifications
--------  -----  --------------     -----------   ------------
gi1/0/1       RX,TX  PD, SN, SD, SC , 4W      172.16.1.1    Disabled
gi1/0/2       TX     PD, SN              172.16.1.1    Disabled
gi1/0/3       RX,TX  PD, SN, SD, SC      None          Disabled
gi1/0/4       RX,TX  D,  SN, SD, SC      automatic     Disabled
```

Example 2 - Display LLDP configuration for port 1.

```
switchxxxxxx#  show lldp configuration gi1/0/1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5 seconds
LLDP packets handling: Filtering
Chassis ID: mac-address
Port State      Optional TLVs     Address      Notifications
---- ---------- --------------    -----------  -----------
gi1/0/1  RX, TX     PD, SN, SD, SC, 4W    72.16.1.1    Disabled
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs
PVID: Enabled
PPVIDs: 0, 1, 92
VLANs: 1, 92
Protocols: 802.1x
```

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

Field	Description
Timer	The time interval between LLDP updates.
Hold multiplier	The amount of time (as a multiple of the timer interval) that the receiving device holds a LLDP packet before discarding it.
Reinit timer	The minimum time interval an LLDP port waits before re-initializing an LLDP transmission.
Tx delay	The delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.

Field	Description
Port	The port number.
State	The port's LLDP state.
Optional TLVs	Optional TLVs that are advertised. Possible values are: PD - Port description SN - System name SD - System description SC - System capabilities 4W - 4 wire spare pair capability
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.

show lldp local

To display the LLDP information that is advertised from a specific port, use the **show lldp local** Privileged EXEC mode command.

Syntax

show lldp local *interface-id*

Parameters

Interface-id— Specifies a port ID.

Default Configuration

N/A.

Command Mode

Privileged EXEC mode

Example

The following examples display LLDP information that is advertised from gi1/0/1 and 2.

```
switchxxxxxx#  show lldp local gi1/0/1
Device ID: 0060.704C.73FF
```

```
Port ID: gi1/0/1
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
Power Type: Type 1 PSE
Power Source: Primary Power Source
Power Priority: Unknown
PSE Allocated Power Value: 30
4-Pair POE supported: Yes
Spare Pair Detection/Classification required: Yes
PD Spare Pair Desired State: Enabled
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 08 00 01 (PAUSE)
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
switchxxxxxx#  show lldp local gi1/0/2
LLDP is disabled.
```

show lldp local tlvs-overloading

When an LLDP packet contains too much information for one packet, this is called overloading. To display the status of TLVs overloading of the LLDP on all ports or on a specific port, use the **show lldp local tlvs-overloading** EXEC mode command.

Syntax

show lldp local tlvs-overloading *[interface-id]*

Parameters

interface-id—(Optional) Specifies a port ID.

Default Configuration

If no port ID is entered, the command displays information for all ports.

Command Mode

User 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

```
switchxxxxxx#  show lldp local tlvs-overloading gi1/0/1
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
```

show lldp med configuration

To display the LLDP Media Endpoint Discovery (MED) configuration for all ports or for a specific port, use the **show lldp med configuration** Privileged EXEC mode command.

Syntax

show lldp med configuration *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies the port ID.

- **detailed**—(Optional) 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

Example 1 - The following example displays the LLDP MED configuration for all interfaces.

```
switchxxxxxx#  show lldp med configuration
Fast Start Repeat Count: 4.
lldp med network-policy voice: manual
Network policy 1
-------------------
Application type: voiceSignaling
VLAN ID: 1  untagged
Layer 2 priority: 0
DSCP: 0
Port    Capabilities   Network Policy Location  Notifications  Inventory
------ -------------- -------------- ---------- -------------   --------
gi1/0/1    Yes             Yes            Yes         Enabled        Yes
gi1/0/2    Yes             Yes            No          Enabled        No
gi1/0/3    No              No             No          Enabled        No
```

Example 2 - The following example displays the LLDP MED configuration for gi1/0/1.

```
switchxxxxxx#  show lldp med configuration gi1/0/1
Port    Capabilities   Network Policy   Location  Notifications Inventory
------- -------------- ---------------- --------- ----------    --------
gi1/0/1     Yes             Yes             Yes       Enabled        Yes
Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

show lldp neighbors

To display information about neighboring devices discovered using LLDP, use the **show lldp neighbors** Privileged EXEC mode command. The information can be displayed for all ports or for a specific port.

Syntax

show lldp neighbors *[interface-id]*

Parameters

interface-id—(Optional) 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.

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.

```
switchxxxxxx#  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
----- ---------------   -------- ----------  -----------  ----
gi1/0/1 00:00:00:11:11:11 gi1/0/1 ts-7800-2 B 90
gi1/0/1 00:00:00:11:11:11 gi1/0/1 ts-7800-2 B 90
gi1/0/2 00:00:26:08:13:24 gi1/0/3 ts-7900-1 B,R 90
gi1/0/3 00:00:26:08:13:24 gi1/0/2 ts-7900-2 W 90
```

Example 2 - The following example displays information about neighboring devices discovered using LLDP on port 1.

```
switchxxxxxx#  show lldp neighbors gi1/0/1
Device ID: 00:00:00:11:11:11
Port ID: gi1/0/1
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
Power Type: Type 1 PSE
Power Source: Primary Power Source
Power Priority: Unknown
PD Requested Power Value: 30
4-Pair POE supported: Yes
Spare Pair Detection/Classification required: Yes
PD Spare Pair Desired State: Enabled
PD Spare Pair Operational State: Enabled
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
LLDP MED	
LLDP MED - Network Policy	
LLDP MED - Power Over Ethernet	
LLDP MED - Location	
Port	The port number.
Device ID	The neighbor device’s configured ID (name) or MAC address.
Port ID	The neighbor device’s port ID.
System name	The neighbor device’s administratively assigned name.

Field	Description
Capabilities	The capabilities discovered on the neighbor device. Possible values are: • B - Bridge • R - Router • W - WLAN Access Point • T - Telephone • D - DOCSIS cable device • H - Host • r - Repeater • O - Other
System description	The neighbor device's system description.
Port description	The neighbor device's port description.
Management address	The neighbor device's management address.
Auto-negotiation support	The auto-negotiation support status on the port. (supported or not supported)
Auto-negotiation status	The active status of auto-negotiation on the port. (enabled or disabled)
Auto-negotiation Advertised Capabilities	The port speed/duplex/flow-control capabilities advertised by the auto-negotiation.
Operational MAU type	The port MAU type.
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, Backup power source. Unknown Power source, PSE and local power source, Local Only power source and PSE only power source.
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.
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.
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.
Coordinates, Civic address, ECS ELIN.	The location information raw data.

show lldp statistics

To display LLDP statistics on all ports or a specific port, use the show **lldp statistics** EXEC mode command.

Syntax

show lldp statistics *[interface-id* | **detailed**]

Parameters

- **interface-id**—(Optional) Specifies the port ID.
- **detailed**—(Optional) 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

User EXEC mode

Example

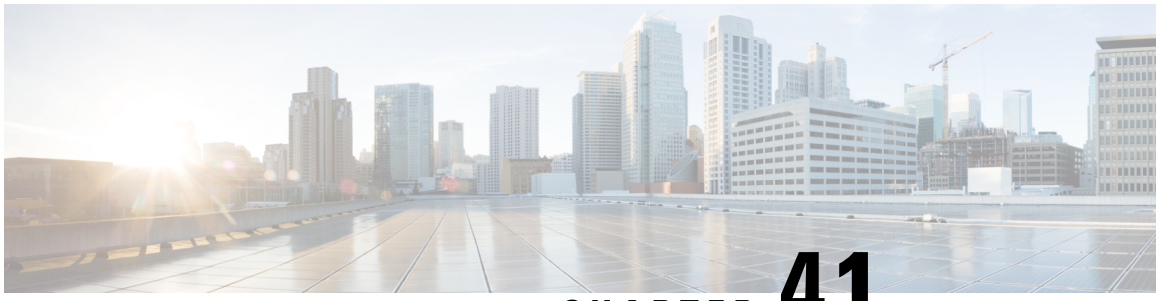
```
switchxxxxxx#  show lldp statistics
Tables Last Change Time: 14-Oct-2010 32:08:18
Tables Inserts: 26
Tables Deletes: 2
Tables Dropped: 0
Tables Ageouts: 1
       TX Frames      RX Frame                RX  TLVs        RX Ageouts
Port  Total Total Discarded Errors   Discarded   Unrecognized  Total
----- ---- ----- --------- --------- ---------   ---------    ------------
gi1/0/1   730   850    0       0         0             0          0
gi1/0/2   0       0    0       0         0             0          0
gi1/0/3   730     0    0       0         0             0          0
gi1/0/4   0       0    0       0         0             0          0
```

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

Field	Description
LLDP MED	
LLDP MED - Power Over Ethernet	
LLDP MED - Location	
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

Field	Description
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.
Capabilities	The sender's LLDP-MED capabilities.
Device type	The device type. Indicates whether the sender is a Network Connectivity Device or Endpoint Device, and if an Endpoint, to which Endpoint Class it belongs.
`LLDP MED - Network Policy`	
Application type	The primary function of the application defined for this network policy.
Flags	Flags. The possible values are: Unknown policy: Policy is required by the device, but is currently unknown. Tagged VLAN: The specified application type is using a Tagged VLAN. Untagged VLAN: The specified application type is using an Untagged VLAN.
VLAN ID	The VLAN identifier for the application.
Layer 2 priority	The Layer 2 priority used for the specified application.
DSCP	The DSCP value used for the specified application.
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.

Field	Description
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.
Coordinates, Civic address, ECS ELIN.	The location information raw data.



CHAPTER 41

Loopback Detection Commands

This chapter contains the following sections:

- loopback-detection enable (Global), on page 663
- loopback-detection enable (Interface), on page 664
- loopback-detection interval, on page 664
- show loopback-detection, on page 665

loopback-detection enable (Global)

To enable the Loopback Detection (LBD) feature globally, use the **loopback-detection enable** Global Configuration mode command. To disable the Loopback Detection feature, use the **no** form of this command.

Syntax

loopback-detection enable

no loopback-detection enable

Parameters

This command has no arguments or keywords.

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.

```
switchxxxxxx(config)#  loopback-detection enable
```

loopback-detection enable (Interface)

To enable the Loopback Detection (LBD) feature on an interface, use the **loopback-detection enable** Interface (Ethernet, Port Channel) Configuration mode command. To disable the Loopback Detection feature on the interface, use the **no** form of this command.

Syntax

loopback-detection enable

no loopback-detection enable

Parameters

This command has no arguments or keywords.

Default Configuration

Loopback Detection is enabled on an interface.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

This command enables Loopback Detection on an interface. Use the **loopback-detection enable** Global Configuration command to enable Loopback Detection globally.

Example

The following example enables the Loopback Detection feature on port gi1/0/4.

```
switchxxxxxx(config)#  interface gi1/0/4
switchxxxxxx(config-if)#  loopback-detection enable
```

loopback-detection interval

To set the time interval between LBD packets, use the **loopback-detection interval** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

loopback-detection interval *seconds*

no loopback-detection interval

Parameters

seconds—Specifies the time interval in seconds between LBD packets. (Range: 10–60 seconds)

Default Configuration

The default time interval between LBD packets is 30 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the time interval between LBD packets to 45 seconds.

```
switchxxxxxx(config)#  loopback-detection interval 45
```

show loopback-detection

To display information about Loopback Detection, use the **show loopback-detection** Privileged EXEC mode command.

Syntax

show loopback-detection [*interface-id* | **detailed**]

Parameters

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

Privileged EXEC mode

User Guidelines

Operational status of Active indicates the following conditions are meet:

- Loopback is globally enabled.
- Loopback is enabled on the interface.
- Interface operational state of the interface is up.
- Interface STP state is Forwarding or STP state is disabled.

Operational status of LoopDetected indicates that the interface entered errDisabled state.

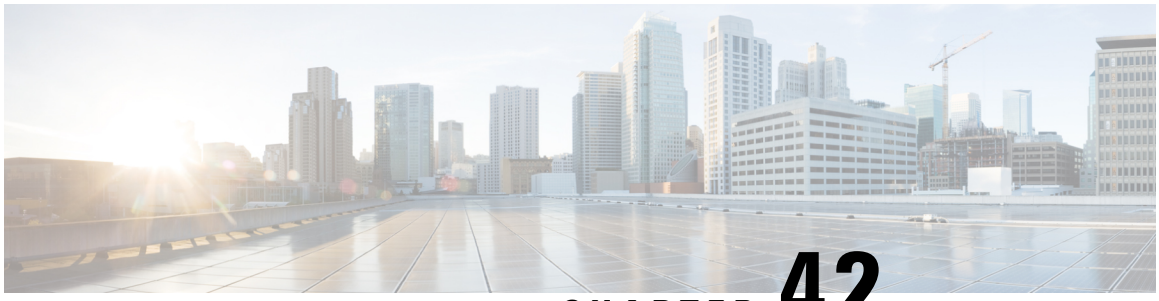
Operational status of Inactive indicates that loopback detection is not actively attempting to detect loops, i.e. the Active status conditions are not meet.

Example

The following example displays information about the status of Loopback Detection.

```
Console# show loopback-detection
Loopback detection: Enabled
LBD packets interval: 30 Seconds
```

Interface	Loopback Detection Admin State	Loopback Detection Operational State
---	---	---
gi1/0/1	Enabled	Active
gi1/0/2	Enabled	LoopDetected
gi1/0/3	Enabled	Inactive
gi1/0/4	Disabled	Inactive



CHAPTER 42

Macro Commands

This chapter contains the following sections:

- macro name, on page 667
- macro, on page 669
- macro description, on page 671
- macro global, on page 672
- macro global description, on page 673
- show parser macro, on page 674

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. 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.

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 these keywords:

- A macro can contain up to three keywords.
- All matching occurrences of the keyword are replaced by the corresponding value specified in the **macro** command.
- 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.

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.)

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)# interface gi1/0/1
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
```

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—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 (Ethernet, Port Channel) 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.

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

```
switchxxxxxx(config)# interface gi1/0/2
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 gi1/0/2
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)# interface gi1/0/1
switchxxxxxx(config-if)# macro trace dup
Applying command...'duplex full'
Applying command...'speed auto'
% bad parameter value
switchxxxxxx(config-if)#
```

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 (Ethernet, Port Channel) 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.

Example

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# macro apply dup
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface gi1/0/3
```

```
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(config)# exit
switchxxxxxx# show parser macro description
Global Macro(s):
Interface      Macro Description(s)
------------   ------------------------------------------------
gi1/0/2             dup
gi1/0/3             duplex | dup | duplex
------------------------------------------------------------
switchxxxxxx# configure
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# no macro description
switchxxxxxx(config-if)# end
switchxxxxxx(config)# exit
switchxxxxxx# show parser macro description
Global Macro(s):
Interface      Macro Description(s)
---------      ------------------------------------------------
gi1/0/3            duplex | dup | duplex
------------------------------------------------------------
```

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—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.

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'
```

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.

Examples

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

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 the **detailed** keyword is not used, only present ports are displayed.

Command Mode

User EXEC mode

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 : company-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
------------------------------------------------------------
Macro name : company-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
```

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.

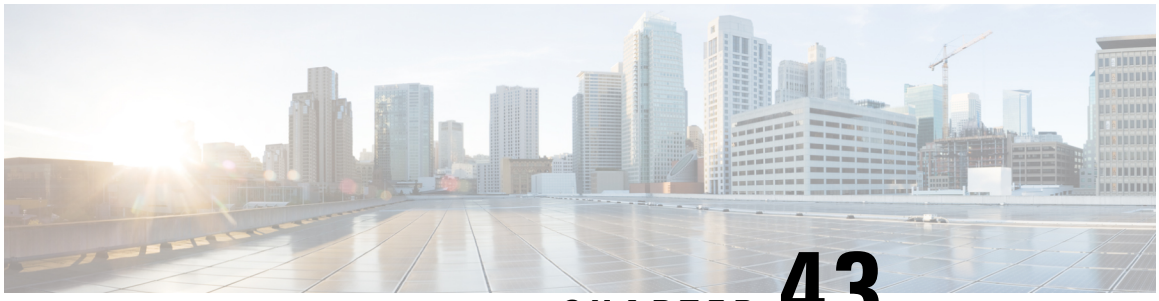
```
switchxxxxxx# show parser macro brief
default global : company-global
default interface: company-desktop
default interface: company-phone
default interface: company-switch
default interface: company-router
customizable : snmp
```

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

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

Example 5 - This is an example of output from the **show parser macro description interface** command.

```
switchxxxxxx# show parser macro description interface gi1/0/2
Interface Macro Description
---------------------------------------------------------------
gi1/0/2 this is test macro
---------------------------------------------------------------
```



CHAPTER 43

Management ACL Commands

This chapter contains the following sections:

- deny (Management), on page 677
- permit (Management), on page 678
- management access-list, on page 679
- management access-class, on page 680
- show management access-list, on page 681
- show management access-class, on page 681

deny (Management)

To set permit rules (ACEs) for the management access list (ACL), use the **deny** Management Access-list Configuration mode command.

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**—(Optional) Specifies an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service*—(Optional) 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
```

permit (Management)

To set permit rules (ACEs) for the management access list (ACL), use the **permit** Management Access-list Configuration mode command.

Syntax

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

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

Parameters

- **interface-id** —(Optional) Specify an interface ID. The interface ID can be one of the following types: Ethernet port, Port-channel or VLAN
- **service** *service* — (Optional) 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
```

management access-list

To configure a management access list (ACL) and enter the Management Access-list Configuration mode, use the **management access-list** Global Configuration mode command. To delete an ACL, use the **no** form of this command.

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, on page 680 command to select the active access list.

The active management list cannot be updated or removed.

A management access-list configured as the access-class for the quiet-mode period (command login quiet-mode access-class in AAA Commands section) cannot be changed 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 1 - The following example creates a management access list called **mlist**, configures management gi1/0/1 and gi1/0/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# permit gi1/0/1
switchxxxxxx(config-macl)# permit gi1/0/9
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

Example 2 - The following example creates a management access list called ‘mlist’, configures all interfaces to be management interfaces except gi1/0/1 and gi1/0/9, and makes the new access list the active list.

```
switchxxxxxx(config)# management access-list mlist
switchxxxxxx(config-macl)# deny gi1/0/1
switchxxxxxx(config-macl)# deny gi1/0/9
switchxxxxxx(config-macl)# permit
switchxxxxxx(config-macl)# exit
switchxxxxxx(config)#
```

management access-class

To restrict management connections by defining the active management access list (ACL), use the **management access-class** Global Configuration mode command. 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
```

show management access-list

To display management access lists (ACLs), use the **show management access-list** Privileged EXEC mode command.

Syntax

show management access-list [*name*]

Parameters

name—(Optional) 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 gi1/0/1 service telnet
! (Note: all other access implicitly denied)
console(config-macl)#
```

show management access-class

To display information about the active management access list (ACLs), use the **show management access-class** Privileged EXEC mode command.

Syntax

show management access-class

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

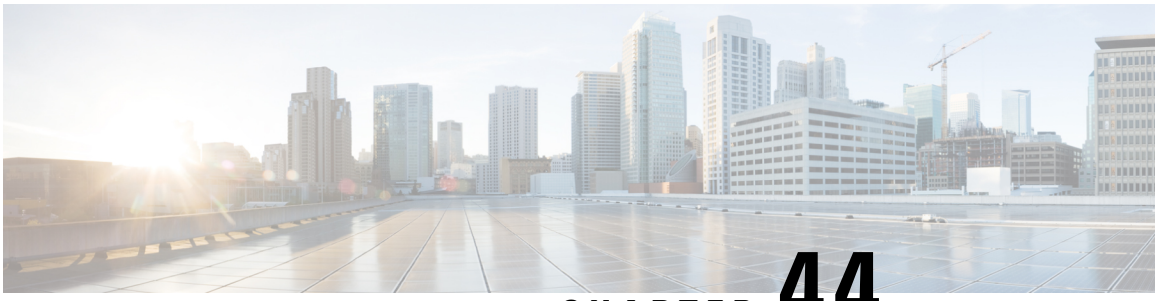
Example

Example 1 -The following example displays the active management ACL information.

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

Example 2 - The following example displays the active management ACL information, when management access class is enabled on the device, and the device is in the quiet-mode period (see commands login block-for and login quiet-mode access-class in AAA Commands section):

```
switchxxxxxx# show management access-class
Management access-class is enabled, using login quiet-mode period
access-class quiet-ACL(mlist access-list will be active when login quiet-mode
period ends
```



CHAPTER 44

MLD Commands

This chapter contains the following sections:

- clear ipv6 mld counters, on page 683
- ipv6 mld last-member-query-count, on page 684
- ipv6 mld last-member-query-interval, on page 684
- ipv6 mld query-interval, on page 685
- ipv6 mld query-max-response-time, on page 686
- ipv6 mld robustness, on page 687
- ipv6 mld version, on page 687
- show ipv6 mld counters, on page 688
- show ipv6 mld groups, on page 689
- show ipv6 mld groups summary, on page 690
- show ipv6 mld interface, on page 691

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***—(Optional) Interface Identifier.

Command Mode

Privileged EXEC mode

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:

```
switchxxxxxx# clear ipv6 mld counters vlan 100
```

ipv6 mld last-member-query-count

To configure the Multicast Listener Discovery (MLD) last member query counter, use the **ipv6 mld last-member-query-count** command in Interface Configuration mode. To restore the default value, use the **no** form of this command.

Syntax

ipv6 mld last-member-query-count count

no ipv6 mld last-member-query-count

Parameters

count—The number of times that group- or group-source-specific queries are sent upon receipt of a message indicating a leave. (Range: 1–7)

Default Configuration

A value of MLD Robustness variable.

Command Mode

Interface Configuration mode

User Guidelines

Use the **ipv6 mld robustness** command to change the MLD last member query counter.

Example

The following example changes a value of the MLD last member query counter to 3:

```
switchxxxxxx(config)# interface vlan 1
ipv6 mld last-member-query-count 3
exit
```

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 mode

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 MLD last member query interval to 1500 milliseconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld last-member-query-interval 1500
switchxxxxxx(config-if)# exit
```

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 30 to 18000.

Default Configuration

The default MLD query interval is 125 seconds.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld query-interval 180
switchxxxxxx(config-if)# exit
```

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: 5–20)

Default Configuration

10 seconds.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld query-max-response-time 8
switchxxxxxx(config-if)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ipv6 mld robustness 3
switchxxxxxx(config-if)# exit
```

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

1

Command Mode

Interface Configuration mode

User Guidelines

Use the command to change the default version of MLD.

Example

The following example configures the router to use MLD Version 1:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld version 1
switchxxxxxx(config-if)# exit
```

show ipv6 mld counters

To display the Multicast Listener Discovery (MLD) traffic counters, use the **show ipv6 mld counters** command in User EXEC mode.

Syntax

show ipv6 mld counters [*interface-id*]

Parameters

- ***interface-id***—(Optional) Interface Identifier.

Command Mode

User EXEC mode

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:

```
switchxxxxxx# 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
```

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 mode.

Syntax

show ipv6 mld groups [**link-local** | *group-name* | *group-address* | *interface-id*] [**detail**]

Parameters

- **link-local**—(Optional) Displays the link-local groups.
- ***group-name* | *group-address***—(Optional) IPv6 address or name of the multicast group.
- ***interface-id***—(Optional) Interface identifier.
- **detail**—(Optional) Displays detailed information about individual sources.

Command Mode

User EXEC mode

User Guidelines

Use the **show ipv6 mld groups** [**detail**] command to display all directly connected groups.

Use the **show ipv6 mld groups link-local** [**detail**] command to display all directly connected link-local groups.

Use the **show ipv6 mld groups** [*group-name* | *group-address*] [**detail**] command to display one given directly connected group.

Use the **show ipv6 mld groups** *interface-id* [**detail**] command to display all groups directly connected to the given interface.

Example 1. The following is sample output from the **show ipv6 mld groups** command. It shows all of the groups joined by VLAN 100:

```
switchxxxxxx# 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:

```
switchxxxxxx# 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
```

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 mode.

Syntax

show ipv6 mld groups summary

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

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:

```
switchxxxxxx# 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.

show ipv6 mld interface

To display multicast-related information about an interface, use the **show ipv6 mld interface** command in User EXEC mode.

Syntax

show ipv6 mld interface [*interface-id*]

Parameters

- ***interface-id***—Interface identifier.

Command Mode

User EXEC mode

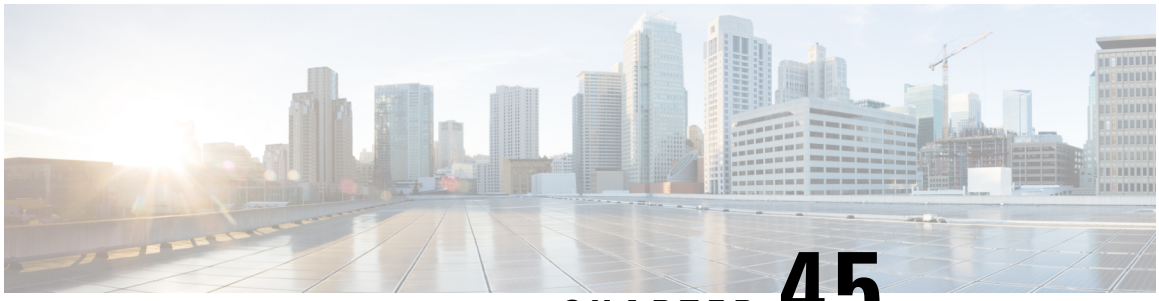
User Guidelines

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:

```
switchxxxxxx# 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
```



CHAPTER 45

MLD Proxy

This chapter contains the following sections:

- ipv6 mld-proxy, on page 693
- ipv6 mld-proxy downstream protected, on page 694
- ipv6 mld-proxy downstream protected interface, on page 695
- ipv6 mld-proxy ssm, on page 695
- show ipv6 mld-proxy interface, on page 696

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 mode

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 1. The following example adds a downstream interface to a MLD Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 mld-proxy vlan 200
switchxxxxxx(config-if)# exit
```

Example 2. The following example adds a range of downstream interfaces to an IGMP Proxy process with vlan 200 as its Upstream interface:

```
switchxxxxxx(config)# interface range vlan 100-105
switchxxxxxx(config-if)# ipv6 mld-proxy vlan 200
switchxxxxxx(config-if)# exit
```

ipv6 mld-proxy downstream protected

To disable forwarding of IPv6 Multicast traffic from downstream interfaces, use the **ipv6 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:

```
switchxxxxxx(config)# ipv6 mld-proxy downstream protected
```

ipv6 mld-proxy downstream protected interface

To disable or enable forwarding of IPv6 Multicast traffic from a given downstream interface, use the **ipv6 mld-proxy downstream protected interface** command in Interface Configuration mode. To return to default, use the **no** form of this command.

Syntax

ipv6 mld-proxy downstream protected interface {enabled | disabled}

no ipv6 mld-proxy downstream protected interface

Parameters

- **enabled**—Downstream interface protection on the interface is enabled. IPv6 Multicast traffic arriving on the interface will not be forwarded.
- **disabled**—Downstream interface protection on the interface is disabled. IPv6 Multicast traffic arriving on the interface will be forwarded.

Default Configuration

Global downstream protection configuration (see the **ipv6 mld-proxy downstream protected** command)

Command Mode

Interface Configuration mode

User Guidelines

Use the **ipv6 mld-proxy downstream protected interface disabled** command to block forwarding from the given downstream interface.

Use the **ipv6 mld-proxy downstream protected interface enabled** command to allow forwarding from the given downstream interface.

The command can be configured only for a downstream interface. When a downstream interface is removed from the MLD Proxy tree the configuration is removed too.

Example

The following example prohibits forwarding from downstream interface vlan 100:

```
switchxxxxxx(config)# interface vlan100
switchxxxxxx(config-if)# ipv6 mld-proxy downstream protected interface enabled
switchxxxxxx(config-if)# exit
```

ipv6 mld-proxy ssm

To define the Source Specific Multicast (SSM) range of IP Multicast addresses, use the **ipv6 mld-proxy ssm** command in Global Configuration mode. To disable the SSM range, use the **no** form of this command.

Syntax

ipv6 mld-proxy ssm {**default** | **range** *access-list*}

no ipv6 mld-proxy ssm

Parameters

default—Defines the SSM range access list to FF3x::/32 (see rfc4607).

range *access-list*—Specifies the standard IPv6 access list name defining the SSM range.

Default Configuration

The command is disabled.

Command Mode

Global Configuration mode

User Guidelines

A new **ipv6 mld-proxyssm** command overrides the previous **ipv6 mld-proxy ssm** command.

Use the **no ipv6 mld-proxy ssm** command 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**:

```
switchxxxxxx(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB8::/64
switchxxxxxx(config)# ipv6 access-list list1 deny FF7E:1220:2001:DB1::1
switchxxxxxx(config)# ipv6 access-list list1 permit FF7E:1220:2001:DB1::/64
switchxxxxxx(config)# ipv6 pim mld-proxy range list1
```

show ipv6 mld-proxy interface

To display information about interfaces configured for MLD Proxy, use the **show ipv6 mld-proxy interface** command in User EXEC mode or Privileged EXEC mode.

Syntax

show ipv6 mld-proxy interface [*interface-id*]

Parameters

- ***interface-id***—(Optional) Display MLD Proxy information about the interface.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The **show ipv6 mld-proxy interface** command is used to display all interfaces where the MLD Proxy is enabled or to display the MLD Proxy configuration for a given interface.

Example 1. The following example displays MLD Proxy status on all interfaces where the MLD Proxy is enabled:

```
switchxxxxxx# 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
Global Downdtream interfaces protection is disabled
SSM Access List Name: list1
Interface  Type         Dicarding IPv6 Multicast
 vlan 100  upstream
*vlan 102  downstream   enabled
*vlan 110  downstream   default
 vlan 113  downstream   disabled
```

Example 2. The following is sample output from the **show ipv6 mld-proxy interface** command for given upstream interface:

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 100
```

* - the switch is the Querier on the interface

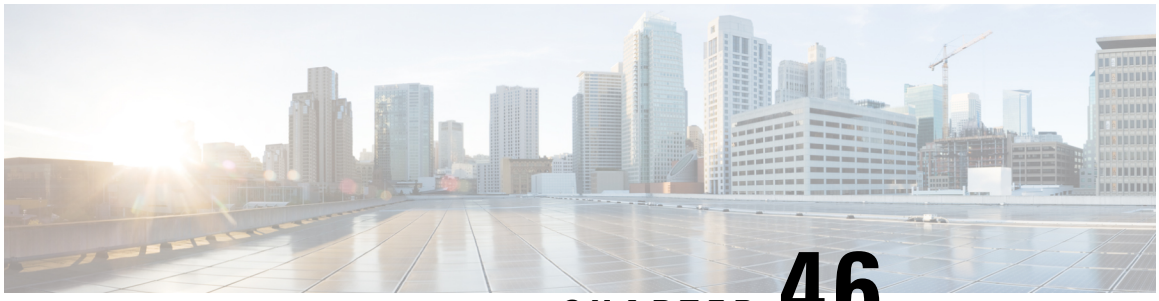
```
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name:
vlan 100 is a Upstream interface
Downstream interfaces:
 *vlan 102, *vlan 110, vlan 113
```

Example 3. The following is sample output from the **show ipv6 mld-proxy interface** command for given downstream interface:

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 102
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is enabled
Global Downdtream interfaces protection is disabled
SSM Access List Name: default
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:

```
switchxxxxxx# show ipv6 mld-proxy interface vlan 1
IPv6 Forwarding is enabled
IPv6 Multicast Routing is enabled
MLD Proxy is disabled
```



CHAPTER 46

MLD Snooping Commands

This chapter contains the following sections:

- ipv6 mld snooping (Global), on page 699
- ipv6 mld snooping vlan, on page 700
- ipv6 mld snooping querier, on page 700
- ipv6 mld snooping vlan querier, on page 701
- ipv6 mld snooping vlan querier election, on page 701
- ipv6 mld snooping vlan querier version, on page 702
- ipv6 mld snooping vlan mrouter , on page 703
- ipv6 mld snooping vlan mrouter interface, on page 704
- ipv6 mld snooping vlan forbidden mrouter, on page 704
- ipv6 mld snooping vlan static, on page 705
- ipv6 mld snooping vlan immediate-leave, on page 706
- show ipv6 mld snooping groups, on page 707
- show ipv6 mld snooping interface, on page 708
- show ipv6 mld snooping mrouter, on page 708

ipv6 mld snooping (Global)

To enable IPv6 Multicast Listener Discovery (MLD) snooping, use the **ipv6 mld snooping** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

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
```

ipv6 mld snooping vlan

To enable MLD snooping on a specific VLAN, use the **ipv6 mld snooping vlan** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 2
```

ipv6 mld snooping querier

To enable globally the MLD Snooping querier, use the **ipv6 mld snooping querier** command in Global Configuration mode. To disable the MLD Snooping querier globally, use the **no** form of this command.

Syntax

ipv6 mld snooping querier

no ipv6 mld snooping querier

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

To run the MLD Snooping querier on a VLAN, you have enable it globally and on the VLAN.

Example

The following example disables the MLD Snooping querier globally:

```
switchxxxxxx(config)# no ipv6 mld snooping querier
```

ipv6 mld snooping vlan querier

To enable the Internet MLD Snooping querier on a specific VLAN, use the **ipv6 mld snooping vlan querier** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *vlan-id* **querier**

no ipv6 mld snooping vlan *vlan-id* **querier**

Parameters

- ***vlan-id***—Specifies the VLAN.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

The MLD Snooping querier can be enabled on a VLAN only if MLD Snooping is enabled for that VLAN.

Example

The following example enables the MLD Snooping querier on VLAN 1:

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 querier
```

ipv6 mld snooping vlan querier election

To enable MLD Querier election mechanism of an MLD Snooping querier on a specific VLAN, use the **ipv6 mld snooping vlan querier election** command in Global Configuration mode. To disable Querier election mechanism, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *vlan-id* **querier election**

no ipv6 mld snooping vlan *vlan-id* **querier election**

Parameters

- ***vlan-id***—Specifies the VLAN.

Default Configuration

Enabled

Command Mode

Global Configuration mode

User Guidelines

Use the **no** form of the **ipv6 mld snooping vlan querier election** command to disable MLD Querier election mechanism on a VLAN.

If the MLD Querier election mechanism is enabled, the MLD Snooping querier supports the standard MLD Querier election mechanism specified in RFC2710 and RFC3810.

If MLD Querier election mechanism is disabled, MLD Snooping Querier delays sending General Query messages for 60 seconds from the time it was enabled. During this time, if the switch did not receive an IGMP query from another Querier - it starts sending General Query messages. Once the switch acts as a Querier, it will stop sending General Query messages if it detects another Querier on the VLAN. In this case, the switch will resume sending General Query messages if it does hear another Querier for Query Passive interval that equals to

<Robustness>*<Query Interval> + 0.5*<Query Response Interval).

It is recommended to disable MLD Querier election mechanism if there is an IPMv6 Multicast router on the VLAN.

Example

The following example disables MLD Snooping Querier election on VLAN 1:

```
switchxxxxxx(config)# no ipv6 mld snooping vlan 1 querier election
```

ipv6 mld snooping vlan querier version

To configure the IGMP version of an IGMP querier on a specific VLAN, use the **ipv6 mld snooping vlan querier version** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *vlan-id* **querier version** {**1** | **2**}

no ipv6 mld snooping vlan *vlan-id* **querier version**

Parameters

- ***vlan-id***—Specifies the VLAN.
- **querier version** {**1** | **2**}—Specifies the MLD version.

Default Configuration

MLDv1.

Command Mode

Global Configuration mode

Example

he following example sets the version of the MLD Snooping Querier VLAN 1 to 2:

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 querier version 2
```

ipv6 mld snooping vlan mrouter

To enable automatic learning of Multicast router ports, use the **ipv6 mld snooping vlan mrouter** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

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

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 mrouter learn pim-dvmrp
```

ipv6 mld snooping vlan mrouter interface

To define a port that is connected to a Multicast router port, use the **ipv6 mld snooping mrouter interface** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-list*

no ipv6 mld snooping vlan *vlan-id* **mrouter interface** *interface-list*

Parameters

- ***vlan-id***—Specifies the VLAN.
- ***interface-list***—Specifies a list of interfaces. The interfaces can be from one of the following types: port or port-channel.

Default Configuration

No ports defined

Command Mode

Global Configuration mode

User Guidelines

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 gi1/0/1
switchxxxxxx(config-if)# ipv6 mld snooping vlan 1 mrouter interface gi1/0/1-4
```

ipv6 mld snooping vlan forbidden mrouter

To forbid a port from being defined as a Multicast router port by static configuration or by automatic learning, use the **ipv6 mld snooping vlan forbidden mrouter** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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 of 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.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 forbidden mrouter interface gi1/0/1
```

ipv6 mld snooping vlan static

To register a IPv6-layer Multicast address to the bridge table, and to add statically ports to the group, use the **ipv6 mld snooping vlan static** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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** *interface-list*—(Optional) 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 FF12::3 gi1/0/1
```

ipv6 mld snooping vlan immediate-leave

To enable MLD Snooping Immediate-Leave processing on a VLAN, use the **ipv6 mld snooping vlan immediate-leave** command in Global Configuration mode. To return to the default, use the **no** form of this command.

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

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.

You can execute the command before the VLAN is created.

Example

```
switchxxxxxx(config)# ipv6 mld snooping vlan 1 immediate-leave
```

show ipv6 mld snooping groups

To display the multicast groups learned by the MLD snooping, use the **show ipv6 mld snooping groups** EXEC mode command in User EXEC mode.

Syntax

show ipv6 mld snooping groups [**vlan** *vlan-id*] [**address** *ipv6-multicast-address*] [**source** *ipv6-address*]

Parameters

- **vlan** *vlan-id*—(Optional) Specifies the VLAN ID.
- **address** *ipv6-multicast-address*—(Optional) Specifies the IPv6 multicast address.
- **source** *ipv6-address*—(Optional) Specifies the IPv6 source address.

Command Mode

User EXEC mode

Default Configuration

Display information for all VLANs and addresses defined on them.

User Guidelines

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 Ports  Exclude Ports  Compatibility Mode
----  -------------  ----------------------  -------------  -------------  ------------------
1     FF12::3        FE80::201:C9FF:FE40:8001 gi1/0/1        gi1/0/2        1
1     FF12::3        FE80::201:C9FF:FE40:8002 gi1/0/2        gi1/0/3        1
19    FF12::8        FE80::201:C9FF:FE40:8003 gi1/0/4                       2
19    FF12::8        FE80::201:C9FF:FE40:8004 gi1/0/1                       2
19    FF12::8        FE80::201:C9FF:FE40:8005 gi1/0/10-11                   2

MLD Reporters that are forbidden statically:
```

VLAN	Group Address	Source Address	Ports
1	FF12::3	FE80::201:C9FF:FE40:8001	gi1/0/3
19	FF12::8	FE80::201:C9FF:FE40:8001	gi1/0/4

show ipv6 mld snooping interface

To display the IPv6 MLD snooping configuration for a specific VLAN, use the **show ipv6 mld snooping interface** EXEC mode command in User EXEC mode.

Syntax

show ipv6 mld snooping interface *vlan-id*

Parameters

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

Default Configuration

Display information for all VLANs.

Command Mode

User 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 Querier is globally enabled
VLAN 1000
  MLD Snooping is enabled
  MLD snooping last immediate leave: enable
  Automatic learning of multicast router ports is enabled
  MLD Snooping Querier is enabled
  MLD Snooping Querier operation state: is running
  MLD Snooping Querier version: 2
  MLD Snooping Querier election is enabled
  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 500 msec
  Groups that are in MLD version 1 compatibility mode:
    FF12::3, FF12::8
```

show ipv6 mld snooping mrouter

To display information on dynamically learned Multicast router interfaces for all VLANs or for a specific VLAN, use the **show ipv6 mld snooping mrouter** EXEC mode command in User EXEC mode.

Syntax

show ipv6 mld snooping mrouter [**interface** *vlan-id*]

Parameters

- **interface** *vlan-id*—(Optional) Specifies the VLAN ID.

Default Configuration

Display information for all VLANs.

Command Mode

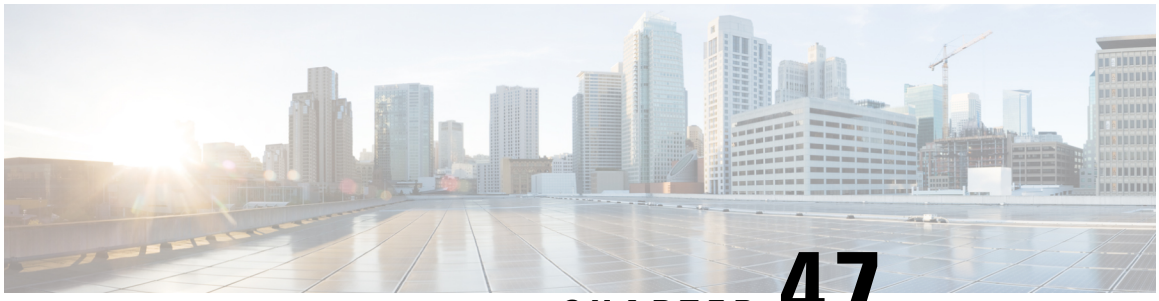
User EXEC mode

Example

The following example displays information on dynamically learned Multicast router interfaces for VLAN 1000:

```
switchxxxxxx# show ipv6 mld snooping mrouter interface 1000
```

VLAN	Dynamic	Static	Forbidden
----	---------	---------	----------
1000	gi1/0/1	gi1/0/2	gi1/0/3-4



CHAPTER 47

OSPF

Refer to the Catalyst 1300X Admin Guide for more information on OSPF feature in Catalyst 1300X series switches.

•

• area authentication, on page 712
• area default-cost, on page 713
• area nssa, on page 714
• area range, on page 716
• area shutdown, on page 717
• area stub, on page 718
• area virtual-link, on page 719
• clear ip ospf process, on page 721
• compatible rfc1583, on page 721
• default-metric (OSPF), on page 722
• ip ospf authentication, on page 723
• ip ospf authentication-key, on page 724
• ip ospf cost, on page 725
• ip ospf dead-interval, on page 726
• ip ospf hello-interval, on page 727
• ip ospf message-digest-key md5, on page 728
• ip ospf mtu-ignore, on page 729
• ip ospf name-lookup, on page 729
• ip ospf passive-interface, on page 730
• ip ospf prefix-suppression, on page 731
• ip ospf priority, on page 732
• ip ospf retransmit-interval, on page 732
• ip ospf shutdown, on page 733
• ip ospf transmit-delay, on page 734
• network area, on page 735
• no area, on page 736
• passive-interface (OSPF), on page 737
• prefix-suppression, on page 738
• redistribute (OSPF), on page 738
• router ospf, on page 741

- router-id, on page 742
- show ip ospf, on page 743
- show ip ospf database, on page 745
- show ip ospf interface, on page 749
- show ip ospf neighbor, on page 751
- show ip ospf router-id, on page 752
- show ip ospf snmp, on page 753
- show ip ospf virtual-links, on page 754
- shutdown (OSPF), on page 755
- snmp-process ospf, on page 755
- snmp-server enable traps ospf, on page 756
- snmp-server enable traps ospf errors, on page 757
- snmp-server enable traps ospf Isa, on page 758
- snmp-server enable traps ospf rate-limit, on page 759
- snmp-server enable traps ospf retransmit, on page 760
- snmp-server enable traps ospf state-change, on page 760

area authentication

To enable area default authentication for an Open Shortest Path First (OSPF) area, use the area authentication command in router configuration mode. To remove a default authentication specification of an area from the configuration, use the no form of this command.

Syntax

area area-id authentication [message-digest]

no area area-id authentication

Parameters

- *area-id*—Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address
- **message-digest**—Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument.

Default Configuration

Type 0 authentication (no authentication).

Command Mode

Router OSPF Configuration mode

User Guidelines

If the area does not exist when the area authentication command is applied it is created.

Specifying default authentication for an area without the message-digest 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, authentication of Type 0 (no authentication) is assumed.

Use the ip ospf authentication interface command to change the area default authentication.

If you enable simple password authentication (type 1), you must configure a password using the ip ospf authentication-key interface command for an IP interface. If a password has not been defined for an IP interface, then OSPF packets are not sent on the interface and received IP interface packets are dropped.

If you configure this command with the message-digest keyword, MD5 authentication is enabled on the IP interfaces (unless it is overridden by the interface level command). in this case a key with a password must be configured using the commmand ip ospf message-digest-key key-id md5. If a md5 digest key has not been defined for an IP interface, then OSPF packets are not sent on the interface and received IP interface packets are dropped.

To remove the default authentication specification for an area, use the no form of this command.



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 mandates default authentication for areas 0 and 10.0.0.0. Authentication keys are also provided:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 10.0.0.0 authentication
switchxxxxxx(config-ospf)# area 0.0.0.0 authentication
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# network 192.168.251.201 area 0.0.0.0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 192.168.251.201
switchxxxxxx(config-ip)# ip ospf authentication-key 12345678
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.56.0.201
switchxxxxxx(config-ip)# ip ospf authentication-key abcdefgh
switchxxxxxx(config-ip)# exit
```

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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# interface vlan1
switchxxxxxx(config-if)# ip address 10.56.0.201 255.255.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# area 10.0.0.0 stub
switchxxxxxx(config-ospf)# area 10.0.0.0 default-cost 20
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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 1.0.0.0 an NSSA area:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# redistribute rip subnets
switchxxxxxx(config-ospf)# network 172.19.92.1 area 1
switchxxxxxx(config-ospf)# area 1.0.0.0 nssa
switchxxxxxx(config-ospf)# exit
```

area range

To consolidate and summarize routes at an area boundary, use the area range command in router this command.

Syntax

area area-id **range** ip-address ip-address-mask **[advertise | not-advertise]**

no area area-id **range** ip-address ip-address-mask

Parameters

- *area-id*—Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IP address.
- *ip-address*—IP Address.
- *ip-address-mask*—IP Address Mask.
- **advertise**—Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). if the **advertise** and **non-advertise** keywords are omitted the **advertise** keyword is assumed.
- **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 OSPF Configuration mode

User Guidelines

If the area does not exist when the area range command is configured it is created.

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.

Multiple area range router configuration commands 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, including **area authentication, 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 36.0.0.0 and for all hosts on network 192.42.110.0:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip address 192.42.110.201 255.255.255.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan102
switchxxxxxx(config-if)# ip address 36.56.1.1 255.255.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# router ospf 201
switchxxxxxx(config-ospf)# network 192.42.110.201 area 0.0.0.0
switchxxxxxx(config-ospf)# network 36.56.1.1 area 36.0.0.0
switchxxxxxx(config-ospf)# area 36.0.0.0 range 10.0.0.0 255.0.0.0
switchxxxxxx(config-ospf)# area 0.0.0.0 range 192.42.110.0 255.255.255.0
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 10.0.0.0 shutdown
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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 ninternal 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:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# network 10.1.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# area 10.0.0.0 default-cost 20
switchxxxxxx(config-ospf)# area 10.0.0.0 stub
switchxxxxxx(config-ospf)# exit
```

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*] [message-digest | null] [message-digest-key

key-id *md5 key-sting*]

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 IPv4 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*—Specifies the time (in seconds) between the hello packets that are sent 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*—Specifies the 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*—Specifies the 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*—Specifies the 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.
- **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
- **message-digest-key** key-id **md5** key-string—
  - *key-id*—A key identifier in the range of 1-255.
  - key-string - Specifies the authentication string. The string can contain from 1 to 16 characters.

Default Configuration

No OSPF virtual link is defined.

Command Mode

Router OSPF Configuration mode

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.



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, including **area authentication, area default-cost, area nssa, area range, area stub, and area virtual-lin**k.

Example

Example 1. The following example establishes a virtual link using by a few commands:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 1.0.0.0 virtual-link 192.168.255.1
switchxxxxxx(config-ospf)# area 1.0.0.0 virtual-link 192.168.255.1 hello-interval 100
switchxxxxxx(config-ospf)# area 1.0.0.0 virtual-link 192.168.255.1 message-digest
message-digest-key 5 md5 myKey
switchxxxxxx(config-ospf)# exit
```

Example 2. The following example establishes a virtual link using bone command:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# area 1.0.0.0 virtual-link 192.168.255.1 hello-interval 100
```

```
message-digest message-digest-key 5 md5 myKey
switchxxxxxx(config-ospf)# exit
```

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 mode

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

```
switchxxxxxx# clear ip ospf process
```

Example 2. The following example restarts one OSP process with process-id 1:

```
switchxxxxxx# clear ip ospf 1 process
```

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the compatible rfc1583 command in router configuration mode. To disable RFC 1583 compatibility, use the no form of this command.

Syntax

compatible rfc1583

no compatible rfc1583

Parameters

N/A

Default Configuration

Compatible with RFC 1583.

Command Mode

Router OSPF Configuration mode

User Guidelines

To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the **no compatible rfc1583** command to enable the calculation method used per RFC 2328.

Example

The following example specifies that the router process is compatible with RFC 1583

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# compatible rfc1583
switchxxxxxx(config-ospf)# exit
```

default-metric (OSPF)

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the default-metric command in router address family topology or 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. The range is from 1 to 4294967295.

Default Configuration

Default metric value appropriate for the specified routing protocol.

Command Mode

Router OSPF Configuration mode

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.



Note When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the redistribute command.

Example

The following example specifies a default metric of 100 for that will used for destributed routes from RIP:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# default-metric 100
switchxxxxxx(config-ospf)# redistribute rip
switchxxxxxx(config-ospf)# exit
```

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 [key-chain *name-of-chain* | **message-digest | null**]

no ip ospf authentication

Parameters

- **key-chain** *name-of-chain* - use the ip ospf authentication key-chain command to specify a key-chain that will be used for authentication. The authentication algorithm type is set using the cryptographic-algorithm command in Key Chain Key Configuration mod.
- **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.

Command Mode

IP Configuration mode

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 type is assumed.

If you enable the simple password authentication, you must configure a password with the ip ospf authentication-key IP interface command. If a password is not defined for the IP interface then OSPF packets are not sent on the IP interface and OSPF packets received on the IP interface are dropped.

If you enable the MD5 authentication, you must configure a key for MD5 authentication using the ip ospf message-digest-key md5 IP interface command. If a key is not defined for the IP interface then OSPF packets are not sent on the IP interface and OSPF packets received on the IP interface are dropped.

If you enable the key-chain option, and the key chain that was specified does not exist, then OSPF packets are not sent on the IP interface and OSPF packets received on the IP interface are dropped.

The authentication algorithm is configured using the cryptographic-algorithm command in Key Chain Key Configuration mode. For more guidelines on cryptographic algorithm key configuration see the user guidelines of the cryptographic-algorithm.

Example

The following example overrides the area default authentication for the 10.56.0.201, 10.10.1.1 and 20.20.1.1 IP interfaces, and keeps the default authentication setting for interface 10.2.1.1:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# area 10.0.0.0 authentication
switchxxxxxx(config-ospf)# network 10.56.0.201 area 10.0.0.0
switchxxxxxx(config-ospf)# network 10.10.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# network 20.20.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# network 10.2.1.1 area 10.0.0.0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 10.56.0.201
switchxxxxxx(config-ip)# ip ospf authentication message-digest
switchxxxxxx(config-ip)# ip ospf message-digest-key 1 md5 key1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.10.1.1
switchxxxxxx(config-ip)# ip ospf authentication null
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 20.20.1.1
switchxxxxxx(config-ip)# ip ospf authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 10.2.1.1
switchxxxxxx(config-ip)# ip ospf authentication-key Ases12@@
switchxxxxxx(config-ip)# exit
```

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 Configuration 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 overrides the previous definition.

Example

The following example shows how to define a password:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf authentication
switchxxxxxx(config-ip)# ip ospf authentication-key alpha$$1267
switchxxxxxx(config-ip)# exit
```

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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf cost 65
switchxxxxxx(config-ip)# exit
```

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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf dead-interval 20
switchxxxxxx(config-ip)# exit
```

ip ospf hello-interval

To specify the interval between hello packets that are sent 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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf hello-interval 15
switchxxxxxx(config-ip)# exit
```

ip ospf message-digest-key md5

To specify the key to be used to generate MD5 digest authentication for the OSPF packets, use the **ip ospf message-digest-key** command in IP interface configuration mode. To remove a key, use the no form of this command.

Syntax

ip ospf message-digest-key *key-id* **md5** *key-string*

no ip ospf message-digest-key *key-id*

Parameters

- *key-id*—A key identifier in the range of 1-255.
- *key-string* - Specifies the authentication string. The string can contain from 1 to 16 characters

Default Configuration

No key exists

Command Mode

Ip Configuration mode

User Guidelines

The key created by this command is used as a “key” to generate the MD5 authentication digest which is then sent in the OSPF packets. A separate key can be assigned to each subnetwork. All neighboring routers on the same subnetwork must have the same key to be able to exchange OSPF information. Only 1 key can be configured per interface.

Use the no form of the command to remove a key.

To update an existing key (of an existing key-id), first remove the existing key using the no form of the command and only then configure the new key.

Example

The following example shows how to enable MD5 authentication on an interface and configure 2 keys which will be used to generate the MD5 digest:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf authentication message-digest
switchxxxxxx(config-ip)# ip ospf message-digest-key 1 md5 key1
switchxxxxxx(config-ip)# exit
```

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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf mtu-ignore
switchxxxxxx(config-ip)# exit
```

ip ospf name-lookup

To configure Open Shortest Path First (OSPF) to look up Domain Name System (DNS) names for use in all OSPF show EXEC command displays, use the ip ospf name-lookup command in global configuration mode. To disable this function, use the no form of this command

Syntax

ip ospf name-lookup

no ip ospf name-lookup

Parameters

N/A

Default Configuration

This command is disabled by default.

Command Mode

Global Configuration mode

User Guidelines

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Example

The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
switchxxxxxx(config)# ip ospf name-lookup
```

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 Configuration mode

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:

```
switchxxxxxx(config)# router ospf 100
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0.0.0.0
switchxxxxxx(config-ospf)# passive-interface
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no ip ospf passive-interface
switchxxxxxx(config-ip)# exit
```

ip ospf prefix-suppression

To prevent OSPF from advertising the interface IP prefix, use the **ip ospf prefix-suppression** command in IP interface configuration mode. To remove the per-interface configuration from the interface and allow the interface to inherit the IP prefix suppression setting from the router configuration, use the **no** form of this command

Syntax

ip ospf prefix-suppression [disable]

no ip ospf prefix-suppression

Parameters

- **disable**—Specifies that OSPF will advertise the interface IP prefix, regardless of the router mode configuration for IP prefix suppression

Default Configuration

Routing updates are sent on the interface.

Command Mode

IP Configuration mode

User Guidelines

Use this command to suppress prefix advertisements for the specified IP interface. This command can also be used to suppress prefixes of passive and Loopback interfaces.

By default, prefix suppression is not configured on an interface. In this case the IP interface will inherit the behavior set by the prefix-suppression router configuration mode command set for the OSPF process. Entering the ip ospf prefix-suppression command will override the prefix-suppression router configuration mode command. Use the command with the disable option to disable all prefix suppression - regardless of the router configuration mode setting.

Example

The following example enables ip prefix suppression on an IP interface:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf prefix-suppression
switchxxxxxx(config-ip)# exit
```

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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf priority 4
switchxxxxxx(config-ip)# exit
```

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.

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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf retransmit-interval 8
switchxxxxxx(config-ip)# exit
```

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

Command Mode

IP Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1
switchxxxxxx(config-ip)# ip ospf shutdown
switchxxxxxx(config-ip)# exit
```

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 Configuration mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf transmit-delay 3
switchxxxxxx(config-ip)# exit
```

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 OSPF Configuration mode

User Gyuidelines

OSPF can be defined only on manually configured IP interfaces, meaning that OSPF 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 OSPF 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:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0.0.0.0
switchxxxxxx(config-ospf)# exit
```

Example 2. The following example enables OSPF on 1.1.1.1 in the shutdown state, configures the interface cost and starts OSPF:

```
switchxxxxxx(config)# router ospf
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0.0.0.0 shutdown
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf cost 102
switchxxxxxx(config-ip)# no ip ospf shutdown
switchxxxxxx(config)# exit
```

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 OSPF Configuration mode

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**. It also removes all of the networks that were associated to that area (**network** ip-address **area** area-id).

Example

The following example removes area 1:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# no area 0.0.0.1
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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 **ip ospf passive-interface disable** 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:

```
switchxxxxxx(config)# router ospf 100
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0.0.0.0
switchxxxxxx(config-ospf)# passive-interface
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# ip ospf passive-interface disable
switchxxxxxx(config-ip)# exit
```

prefix-suppression

To prevent OSPF from advertising all IP prefixes for a specific OSPF process except for prefixes that are associated with loopback and passive interfaces, use the **prefix-suppression** command in router configuration mode. To advertise all IP prefixes, use the **no** form of this command.

Syntax

prefix-suppression

no prefix-suppression

Parameters

N/A

Default Configuration

All IP prefixes are advertised.

Command Mode

Router OSPF Configuration mode

User Guidelines

Use the **prefix-suppression** router configuration mode command to globally suppress advertisement of all IP prefixes (except for prefixes that are associated with loopbacks and passive interfaces) for an entire OSPF process.You can also suppress a specific IP prefix by using the **ip ospf prefix-suppression** command in IP interface configuration mode. When the ip ospf **prefix-suppression** command is configured, it takes precedence over the prefix-suppression router configuration command

Example

The following example globally suppresses all IP prefixes or OSPF process 613 except for prefixes that are associated with loopbacks and passive interfaces:

```
switchxxxxxx(config)# router ospf 613
switchxxxxxx(config-ospf)# network 1.1.1.1 area 0.0.0.0
switchxxxxxx(config-ospf)# prefix-suppression
switchxxxxxx(config-ospf)# exit
```

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, or ospf**.
- *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
    1. the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process.
    2. 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 OSPF Configuration mode

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.

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:

```
switchxxxxxx(config)# router ospf 110
switchxxxxxx(config-ospf)# redistribute rip metric 200 subnets
switchxxxxxx(config-ospf)# exit
```

Example 2. 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):

```
switchxxxxxx(config)# interface vlan 2 0
switchxxxxxx(config-if)# ip address 172.16.0.1 255.0.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 10
switchxxxxxx(config-if)# ip address 10.0.0.1 255.0.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# router ospf 2
switchxxxxxx(config-ospf)# network 172.16.0.1 area 0.0.0.0
switchxxxxxx(config-ospf)# exit
switchxxxxxx(config)# interface ip 172.16.0.1
switchxxxxxx(config-ip)# ip ospf cost 100
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# network 10.0.0.1 area 0.0.0.0
switchxxxxxx(config-ospf)# redistribute ospf 2 subnet
switchxxxxxx(config-ospf)# exit
```

Example 3. 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:

```
switchxxxxxx(config)# router ospf 2
switchxxxxxx(config-ospf)# redistribute ospf 1 match internal metric-type 1
subnet
switchxxxxxx(config-ospf)# redistribute ospf 1 match external-1 metric-type 1
metric 100 subnet
switchxxxxxx(config-ospf)# redistribute ospf 1 match external-2 metric-type 2
metric 200 subnet
switchxxxxxx(config-ospf)# exit
```

Example 4. The following example removes the subnets options:

```
switchxxxxxx(config)# router ospf 2
switchxxxxxx(config-ospf)# no redistribute ospf subnets
switchxxxxxx(config-ospf)# exit
```

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 mode

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:

```
switchxxxxxx(config)# router ospf 2
```

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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# router-id 10.1.1.1
switchxxxxxx(config-ospf)# exit
```

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 mode

Privileged EXEC mode

Example

Example The following is sample output from the show ip ospf command:

```
switchxxxxxx# 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
```

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 [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*]] d**atabase [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*]] d**atabase [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 mode

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:

```
switchxxxxxx# show ip ospf database
OSPF Routing Process 300 with ID 192.168.239.66
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
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
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:

```
switchxxxxxx# show ip ospf database asbr-summary
OSPF Routing Process 300 with ID 192.168.239.66
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:

```
switchxxxxxx# show ip ospf database external
OSPF Routing Process 300 with ID 192.168.239.66
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:

```
switchxxxxxx# show ip ospf database network
OSPF Routing Process 300 with ID 192.168.239.66
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:

```
switchxxxxxx# show ip ospf database router
OSPF Routing Process 300 with ID 192.168.239.66
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:

```
switchxxxxxx# show ip ospf database summary
OSPF Routing Process 300 with ID 192.168.239.66
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:

```
switchxxxxxx# show ip ospf database database-summary
OSPF Routing Process 1 with ID 10.0.1.1
Area 0.0.0.0 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

```
switchxxxxxx# show ip ospf database nssa-external
OSPF Routing Process 300 with ID 192.168.239.66
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
```

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 specifiedrouting 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

User Exec mode

Privileged EXEC mode

Example

Example 1. The following is sample output from the **show ip ospf** interface command when IP interface 192.168.254.202 is specified

```
switchxxxxxx# show ip ospf interface 192.168.254.202
OSPF Routing Process 1 with ID 192.168.0.0
Internet Address 192.168.254.202/24, Area 0.0.0.0
Interface VLAN 10, BROADCAST is up, IP Interface is up, OSPF Adminastrative state is up
Cost: 10
IP Interface has message digest authentication, key id is 1
Prefix-suppression is enabled (global)
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
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 0.0.0.0
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
Neighbor Count is 3, Adjacent neighbor count is 0
Internet Address 192.168.250.202/24, Area 0.0.0.0
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 0.0.0.0
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 0.0.0.0
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:

```
switchxxxxxx# 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
```

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 [detail | interface** *ip-address [neighbor-id]* [**detail**] | *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 router ID in A.B.C.D format.
- **detail**—Displays all neighbors information in detail.

Command Mode

Privileged EXEC mode

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:

```
switchxxxxxx# 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:

```
switchxxxxxx# 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:

```
switchxxxxxx# 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:
switchxxxxxx# 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 :

```
switchxxxxxx# 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
```

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 ip 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.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

N/A

Example

The following is sample output from the show ip ospf router-id command:

```
switchxxxxxx# 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
```

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

User EXEC mode

Privileged EXEC mode

User Guidelines

Use the **show ipv ospf snmp** command to display the OSPF snmp configuration.

Example

The following is sample output from the **show ip ospf snmp** command:

```
switchxxxxxx# 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
```

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

User EXEC mode

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:

```
switchxxxxxx# 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 id is 1
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
```

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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# router ospf 1
switchxxxxxx(config-ospf)# shutdown
switchxxxxxx(config-ospf)# exit
```

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

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:

```
switchxxxxxx(config)# snmp-process ospf 100
```

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 mode

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 example globally enables SNMP notifications for OSPF:

```
switchxxxxxx(config)# snmp-server enable traps ospf
```

snmp-server enable traps ospf errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) errors, use the **snmp-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.
- **virt-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 mode

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:

```
switchxxxxxx(config)# snmp-server enable traps ospf errors
```

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 mode

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.

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

```
switchxxxxxx(config)# snmp-server enable traps ospf lsa lsa-originate
```

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

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 mode

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

The following example sets the trap rate limit window so that during a 40-second window of time, no more that 50 traps are sent:

```
switchxxxxxx(config)# snmp-server enable traps ospf rate-limit 40 50
```

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 mode

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:

```
switchxxxxxx(config)# snmp-server enable traps ospf retransmit virt-packets
```

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 mode

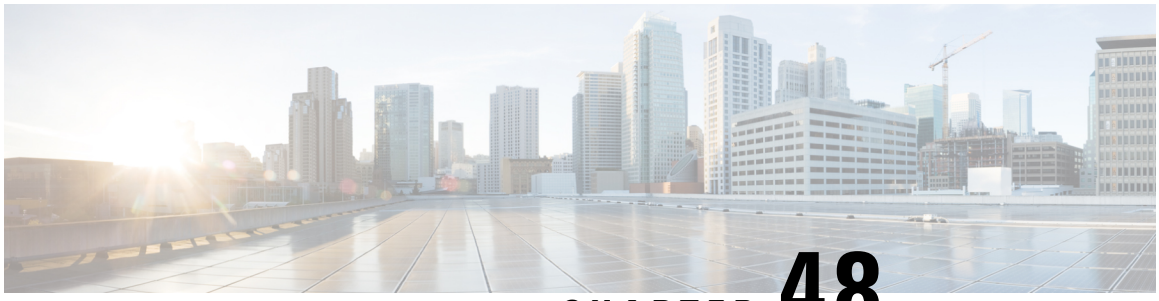
User Guidelines

To enable all traps for transition state changes, enter the **snmp-server enable traps ospf state-change** 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:

```
switchxxxxxx(config)# snmp-server enable traps ospf state-change virtif-state-change
virtneighbor-state-change
```



CHAPTER 48

OSPFv3 Commands

Refer to the Catalyst 1300X Admin Guide for more information on OSPF feature in Catalyst 1300X series switches.

-
- area default-cost, on page 764
- area filter-list, on page 765
- area nssa, on page 766
- area range, on page 767
- area shutdown, on page 768
- area stub, on page 769
- area virtual-link, on page 770
- clear ipv6 ospf process, on page 772
- default metric IPv6 OSPF, on page 772
- ipv6 ospf area, on page 773
- ipv6 ospf cost, on page 774
- ipv6 ospf dead-interval, on page 775
- ipv6 ospf hello-interval, on page 775
- ipv6 ospf mtu-ignore, on page 776
- ipv6 ospf name-lookup, on page 777
- ipv6 ospf prefix-suppression, on page 777
- ipv6 ospf priority, on page 778
- ipv6 ospf retransmit-interval, on page 779
- ipv6 ospf shutdown, on page 780
- ipv6 ospf transmit-delay, on page 781
- ipv6 router ospf, on page 781
- log-adjacency-changes ipv6, on page 782
- no area, on page 783
- passive-interface ipv6, on page 784
- prefix-suppression, on page 785
- redistribute (OSPFv3), on page 785
- router-id IPv6, on page 788
- show ipv6 ospf, on page 788
- show ipv6 ospf database, on page 791
- show ipv6 ospf interface, on page 796

- show ipv6 ospf neighbor, on page 797
- show ipv6 ospf router-id, on page 798
- show ipv6 ospf snmp, on page 799
- show ipv6 ospf virtual-links, on page 800
- shutdown ipv6 ospf, on page 801
- snmp-process ipv6 ospf, on page 802
- snmp-server enable traps ipv6 ospf errors, on page 802
- snmp-server enable traps ipv6 ospf rate-limit, on page 803
- snmp-server enable traps ipv6 ospf state-change, on page 804

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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# area 10.0.0.0 stub
switchxxxxxx(config-ospf)# area 10.0.0.0 default-cost 20
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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 3LSA 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 1.0.0.0:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# area 1.0.0.0 filter-list prefix AREA_1 in
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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 1.0.0.0 an NSSA area:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# area 1.0.0.0 nssa
switchxxxxxx(config-ospf)# exit
```

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** *ipv6-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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 enable
switchxxxxxx(config-if)# ipv6 ospf 1 area 1.0.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# router-id 192.168.255.5
switchxxxxxx(config-ospf)# area 1.0.0.0 range 2001:0DB8:0:1::/64
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# area 10.0.0.0 shutdown
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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 ninternal 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:

```
switchxxxxxx(config)# ipv6 router ospf
switchxxxxxx(config-ospf)# area 10.0.0.0 default-cost 20
switchxxxxxx(config-ospf)# area 10.0.0.0 stub
switchxxxxxx(config-ospf)# exit
```

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 IPv4 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*—Specifies the time (in seconds) between the hello packets that are sent 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*—Specifies the 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*—Specifies the 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*—Specifies the 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 OSPF Configuration mode

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, including **area authentication, 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:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# area 1.0.0.0 virtual-link 192.168.255.1
switchxxxxxx(config-ospf)# exit
```

Example 2. The following example establishes a virtual link in OSPF for IPv6:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# area 1.0.0.0 virtual-link 192.168.255.1 hello-interval 5
switchxxxxxx(config-ospf)# exit
```

clear ipv6 ospf process

•

To restart the Open Shortest Path First (OSPF) process, use the clear ip 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 mode

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

```
switchxxxxxx# clear ipv6 ospf process
```

Example 2. The following example restarts one OSP process with process-id 1:

```
switchxxxxxx# clear ipv6 ospf 1 process
```

default metric IPv6 OSPF

•

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

[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 1-65535
- *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 mode

User Guidelines

Before you enable OSPF for IPv6 on an interface using the ipv6 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:

```
switchxxxxxx(config)# ipv6 unicast-routing
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 enable
switchxxxxxx(config-if)# ipv6 ospf 1 area 0.0.0.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 200
```

```
switchxxxxxx(config-if)# ipv6 enable
switchxxxxxx(config-if)# ipv6 ospf 120 area 1.0.0.0.4.20.9
switchxxxxxx(config-if)# exit
```

ipv6 ospf cost

•

To explicitly specify the cost of sending a packet on an interface, use the ipv6 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

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

IP Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 200
switchxxxxxx(config-if)# ipv6 ospf cost 65
switchxxxxxx(config-if)# exit
```

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 **ip ospf hello-interval** command.

Command Mode

IP Configuration mode

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 60 seconds:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 ospf dead-interval 60
switchxxxxxx(config-if)# exit
```

ipv6 ospf hello-interval

To specify the interval between hello packets that are sent 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

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

IP Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ipv6 ospf hello-interval 15
switchxxxxxx(config-if)# exit
```

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 ip ospf mtu-ignore command in IP 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 mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-if)# ipv6 ospf mtu-ignore
switchxxxxxx(config-if)# exit
```

ipv6 ospf name-lookup

To display Open Shortest Path First (OSPF) router IDs as Domain Naming System (DNS) names, use the ipv6 ospf name-lookup command in global configuration mode. To stop displaying OSPF router IDs as DNS names, use the no form of this command.

Syntax

ipv6 ospf name-lookup

no ipv6 ospf name-lookup

Parameters

This command has no arguments or keywords.

Default Configuration

This command is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Example

The following example disables MTU mismatch detection on receiving DBD packets:

```
switchxxxxxx(config)# ipv6 ospf name-lookup
```

ipv6 ospf prefix-suppression

To prevent OSPF from advertising the interface IPv6 prefixes, use the ipv6 ospf prefix-suppression command in interface configuration mode. To remove the per-interface configuration from the interface and allow the

interface to inherit the IP prefix suppression setting from the router configuration, use the no form of this command:

Syntax

ipv6 ospf prefix-suppression [disable]

no ipv6 ospf prefix-suppression

Parameters

- **disable**—Specifies that OSPF will advertise the interface IP prefix, regardless of the router mode configuration for IP prefix suppression

Default Configuration

Routing updates are sent on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use this command to suppress Ipv6 prefix(es) advertisements for the interface. This command can also be used to suppress prefixes of passive and Loopback interfaces.

By default, IPv6 prefix suppression is not configured on an interface. In this case the interface will inherit the behavior set by the prefix-suppression router configuration mode command set for the OSPFv3 process. Entering the ipv6 ospf prefix-suppression command will override the prefix-suppression router configuration mode command. Use the command with the disable option to disable all ipv6 prefix suppression on the interface - regardless of the router configuration mode setting.

Example

The following example enables ip prefix suppression on an interface VLAN 100:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-ip)# ip ospf prefix-suppression
switchxxxxxx(config-ip)# exit
```

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 mode

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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-if)# ipv6 ospf priority 4
switchxxxxxx(config-if)# exit
```

ipv6 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

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 mode

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.

Example

The following example sets the retransmit interval value to 8 seconds:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-if)# ipv6 ospf retransmit-interval 8
switchxxxxxx(config-if)# exit
```

ipv6 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

This command has no arguments or keywords.

Default Configuration

This command is disabled.

Command Mode

Interface Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip ospf shutdown
switchxxxxxx(config-if)# exit
```

ipv6 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

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 mode

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:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-ip)# ipv6 ospf transmit-delay 3
switchxxxxxx(config-ip)# exit
```

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 65535. 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 mode

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:

```
switchxxxxxx(config)# ipv6 router ospf 1
```

log-adjacency-changes ipv6

To configure the router to send a syslog message when an Open Shortest Path First (OSPF) for IPv6 neighbor goes up or down, use the log-adjacency-changes command in router configuration mode. To turn off this function, use the no form of this command.

Syntax

log-adjacency-changes [detail]

no log-adjacency-changes

Parameters

- **detail**—Sends a syslog message for each state change, not just when a neighbor goes up or down.

Default Configuration

Enabled

Command Mode

Router OSPF Configuration mode

User Guidelines

This command allows you to know about OSPF neighbors going up or down. The log-adjacency-changes command provides a high level view of those changes of the peer relationship. The log-adjacency-changes command is on by default but only up/down (full/down) events are reported, unless the detail keyword is also used.

Example

The following example configures the router to send a syslog message when an OSPF neighbor state changes:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# log-adjacency-changes detail
switchxxxxxx(config-ospf)# exit
```

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 OSPF Configuration mode

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**. It also removes all of the networks that were associated to that area (**network** ip-address **area** area-id).

Example

The following example removes area 1:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# no area 0.0.0.1
switchxxxxxx(config-ospf)# exit
```

passive-interface ipv6

To disable sending routing updates on an interface, use the passive-interface command in routerconfiguration 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 OSPF Configuration mode

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:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# passive-interface default
switchxxxxxx(config-ospf)# no passive-interface vlan100
switchxxxxxx(config-ospf)# exit
```

prefix-suppression

To prevent OSPFV3 from advertising all IP prefixes for a specific OSPFv3 process except for prefixes that are associated with Loopback and passive interfaces, use the prefix-suppression command in router configuration mode. To advertise all IPv6 prefixes, use the no form of this command.

Syntax

prefix-suppression

no prefix-suppression

Parameters

N/A

Default Configuration

All IPv6` prefixes are advertised.

Command Mode

Router OSPF Configuration mode

User Guidelines

Use the prefix-suppression router configuration mode command to globally suppress advertisement of all IPv6 prefixes (except for prefixes that are associated with loopbacks and passive interfaces) for an entire OSPFv3 process.You can also suppress a specific IPv6 prefix by using the ipv6 ospf prefix-suppression command in IPv6 interface configuration mode. When the ipv6 ospf prefix-suppression command is configured, it takes precedence over the prefix-suppression router configuration command

Example

The following example globally suppresses all IPv6 prefixes for OSPFv3 process 248 except for prefixes that are associated with loopbacks and passive interfaces:

```
switchxxxxxx(config)# ipv6 router ospf 248
switchxxxxxx(config-ospf)# prefix-suppression
switchxxxxxx(config-ospf)# exit
```

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, or ospf.
- *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:

  - from OSPF
    1. the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process.
    2. the external OSPF metric from the redistribution source process is advertised as the external metric with value of 1.
  - from any protocol except OSPF - 20

- metric-type type-value— Used only together with the ospf keywordSpecifies 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 pe 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 mode

Router OSPF Configuration mode

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.

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.

Example

The following example redistributes OSPF 100 for IPv6 routes into the OSPF for IPv6 routing process 1:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# redistribute ospf 100 metric 32 metric-type 1
switchxxxxxx(config-ospf)# exit
```

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*

no router-id

Parameters

- *ipv4-address*—Router ID in IPv4 address format.

Default Configuration

The minimum IPv4 address configured on the router.

Command Mode

Router OSPF Configuration mode

User Guidelines

You can configure an arbitrary value in the IP address. However, each router ID must be unique.

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.

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 ipv6 ospf process command.

Example

The following example specifies a fixed router ID:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# router-id 10.1.1.1
switchxxxxxx(config-ospf)# exit
```

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

N/A

Command Mode

User EXEC mode

Privileged EXEC mode

Example

The following is sample output from the show ipv6 ospf command:

```
switchxxxxxx# show ipv6 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
```

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**

show ipv6 ospf [*process-id [area-id]*] **database adv-router router-id**

show ipv6 ospf [*process-id [area-id]*] **database database-summary**

show ipv6 ospf [*process-id [area-id]*] **database external**

show ipv6 ospf [*process-id [area-id]*] **database grace**

show ipv6 ospf [*process-id [area-id]*] **database inter-area-prefix**

show ipv6 ospf [*process-id [area-id]*] **database inter-area router**

show ipv6 ospf [*process-id [area-id]*] **database link**

show ipv6 ospf [*process-id [area-id]*] **database network**

show ipv6 ospf [*process-id [area-id]*] **database nssa-external**

show ipv6 ospf [*process-id [area-id]*] **database prefix**

show ipv6 ospf [*process-id [area-id]*] **database [router**]

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.
- **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.**network**—Displays information only about the network LSAs.
- *destination-router-id*—The specified destination router ID.
- **link**—Displays information only about the router 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

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

N/A

Example

Example 1. The following is sample output from the show ipv6 ospf database command when no arguments or keywords are used:

```
switchxxxxxx# show ipv6 ospf database
OSPFv3 Router with ID (172.16.4.4) (Process ID 1)
Router Link States (Area 0.0.0.0)
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 0.0.0.0)
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 0.0.0.0)
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 0.0.0.0)
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 0.0.0.0)
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 keyword:

```
switchxxxxxx# show ipv6 ospf database router
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
Router Link States (Area 0.0.0.0)
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:

```
switchxxxxxx# show ipv6 ospf database network
Router Link States (Area 0.0.0.1)
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
Net Link States (Area 0.0.0.1)
ADV Router Age Seq# Attached Router
172.16.6.6 419 0x80000001 172.16.6.3
172.16.6.6 239 0x80000001 172.16.6.6
```

Example 4. The following is sample output from the show ipv6 ospf database command with the link self-originate keywords:

```
switchxxxxxx# show ipv6 ospf database link
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
Link (Type-8) Link States (Area 0.0.0.0)
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 keyword:

```
switchxxxxxx# show ipv6 ospf database prefix
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
Intra Area Prefix Link States (Area 0.0.0.0)
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 keyword

```
switchxxxxxx# show ipv6 ospf database inter-area-prefix
OSPF Routing Process 1 with ID 1.1.1.1
Router Link States(Area 0.0.0.1)
ADV Router Age Seq# Fragment ID Link count Bits
1.1.1.1 510 0x80000004 0 1 E
2.2.2.2 506 0x8000000a 0 1 B
Network Link States(Area 0.0.0.1)
ADV Router Age Seq# Attached Router
2.2.2.2 511 0x80000001 1.1.1.1
2.2.2.2 511 0x80000001 2.2.2.2
Type8 Link States(Area 0.0.0.1)
ADV Router Age Seq# Link ID Interface
1.1.1.1 510 0x80000001 gi1/0/1
Type8 Link States(Area 0.0.0.1)
ADV Router Age Seq# Link ID Interface
2.2.2.2 960 0x80000006 gi1/0/1
```

Example 7. The following is sample output from the show ipv6 ospf database command with the inter-area-router keyword:

```
switchxxxxxx# show ipv6 ospf database inter-area-router
OSPF Routing Process 1 with ID 1.1.1.1
Router Link States(Area 0.0.0.1)
ADV Router Age Seq# Fragment ID Link count Bits
1.1.1.1 514 0x80000004 0 1 E
2.2.2.2 510 0x8000000a 0 1 B
Network Link States(Area 0.0.0.1)
ADV Router Age Seq# Attached Router
2.2.2.2 515 0x80000001 1.1.1.1
```

```
2.2.2.2 515 0x80000001 2.2.2.2
Type8 Link States(Area 0.0.0.1)
ADV Router Age Seq# Link ID Interface
1.1.1.1 514 0x80000001 gi1/0/1
Type8 Link States(Area 0.0.0.1)
ADV Router Age Seq# Link ID Interface
2.2.2.2 964 0x80000006 gi1/0/1
```

Example 8. The following is sample output from the show ipv6 ospf database command with the external keyword:

```
switchxxxxxx# 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:

```
switchxxxxxx# show ipv6 ospf 1 database
OSPFv3 Router with ID (10.2.2.2) (Process ID 1)
Router Link States (Area 0.0.0.0)
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 0.0.0.0)
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 0.0.0.0)
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 0.0.0.0)
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:

```
switchxxxxxx# show ipv6 ospf database grace
OSPF Routing Process 1 with ID 1.1.1.1
Router Link States(Area 0.0.0.1)
ADV Router Age Seq# Fragment ID Link count Bits
1.1.1.1 498 0x80000004 0 1 E
2.2.2.2 494 0x8000000a 0 1 B
Network Link States(Area 0.0.0.1)
ADV Router Age Seq# Attached Router
2.2.2.2 499 0x80000001 1.1.1.1
2.2.2.2 499 0x80000001 2.2.2.2
Type8 Link States(Area 0.0.0.1)
ADV Router Age Seq# Link ID Interface
1.1.1.1 498 0x80000001 gi1/0/1
```

```
Type8 Link States(Area 0.0.0.1)
ADV Router Age Seq# Link ID Interface
2.2.2.2 948 0x80000006 gi1/0/1
```

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 ipv6 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.

Command Mode

User EXEC mode

Privileged EXEC mode

Example

Example 1. The following is sample output from the show ipv6 ospf interface command:

```
switchxxxxxx# show ipv6 ospf interface
tunnel 1 is up
Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
Area 1.0.0.0, 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,
Prefix-suppression is enabled
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 1.0.0.0, 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
```

```
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 1.0.0.0, 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.
```

Example 2. The following sample output from the show ipv6 ospf interface brief command shows a summary of information:

```
switchxxxxxx# 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
```

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 ipv6 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 isenabled.
- *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).

Command Mode

User EXEC mode

Privileged EXEC mode

Example

Example 1. The following is sample output from the show ipv6 ospf neighbor command:

```
switchxxxxxx# 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:

```
switchxxxxxx# show ipv6 ospf neighbor detail
Neighbor 172.16.4.4
In the area 0.0.0.0 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 172.16.3.3
In the area 1.0.0.0 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 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
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.
```

Example 3. The following is sample output from the show ipv6 ospf neighbor command with the detail keyword, displaying graceful-restart information:

```
switchxxxxxx# show ipv6 ospf neighbor detail
Neighbor 10.1.1.1
In the area 0.0.0.0 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
```

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.

Command Mode

User EXEC mode

Privileged EXEC mode

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:

```
switchxxxxxx# 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
```

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

User EXEC mode

Privileged EXEC mode

User Guidelines

Use **the show ipv6 ospf snmp** command to display the OSPF snmp configuration

Example

The following is sample output from the show ipv6 ospf snmp command:

```
switchxxxxxx# show ipv6 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
Virtual Link Bad Packet Notifications are enabled
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
```

show ipv6 ospf virtual-links

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

This command has no arguments or keywords.

Command Mode

User EXEC mode

Privileged EXEC mode

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:

```
switchxxxxxx# 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 the significant 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:

```
switchxxxxxx# 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 1.0.0.0, 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 1.0.0.0, 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)
```

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

This command has no arguments or keywords.

Default Configuration

OSPF stays active under the current instance.

Command Mode

Router OSPF Configuration mode

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:

```
switchxxxxxx(config)# ipv6 router ospf 1
switchxxxxxx(config-ospf)# shutdown
switchxxxxxx(config-ospf)# exit
```

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

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:

```
switchxxxxxx(config)# snmp-process ipv6 ospf 100
```

snmp-server enable traps ipv6 ospf errors

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) errors, use the snmp-server enable traps ipv6 ospf errors command in global configuration mode. To disable SNMP notifications for OSPF errors, use the no form of thiscommand.

Synatx

snmp-server enable traps ipv6 ospf errors [bad-packet] [virt-bad-packet]

no snmp-server enable traps ipv6 ospf errors [bad-packet][virt-bad-packet]

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.
- **virt-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 mode

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:

```
switchxxxxxx(config)# snmp-server enable traps ipv6 ospf errors
```

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

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 mode

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

The following example sets the trap rate limit window so that during a 40-second window of time, no more that 50 traps are sent:

```
switchxxxxxx(config)# snmp-server enable traps ipv6 ospf rate-limit 40 50
```

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 mode

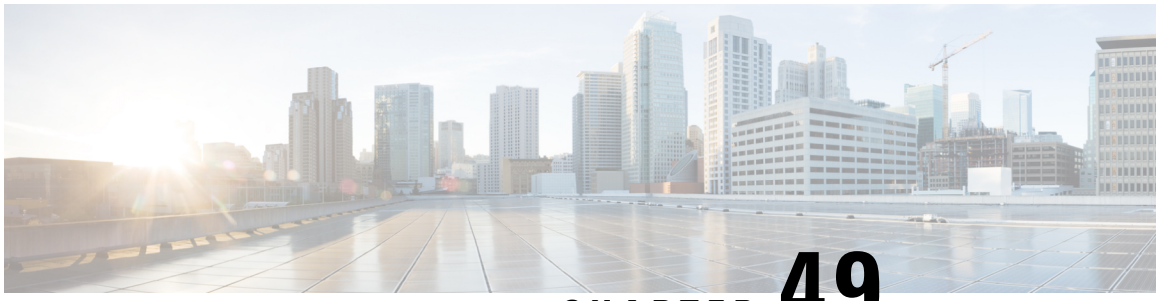
User Guidelines

To enable all traps for transition state changes, enter the snmp-server enable traps ipv6 ospf state-change 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:

```
switchxxxxxx(config)# snmp-server enable traps ipv6 ospf state-change virtif-state-change
virtneighbor-state-change
```



CHAPTER 49

PHY Commands

This chapter contains the following sections:

- test cable-diagnostics tdr, on page 807
- show cable-diagnostics tdr, on page 808
- show cable-diagnostics cable-length, on page 808
- show fiber-ports optical-transceiver, on page 809

test cable-diagnostics tdr

To use Time Domain Reflectometry (TDR) technology to diagnose the quality and characteristics of a copper cable attached to a port, use the **test cable-diagnostics tdr** Privileged EXEC mode command.

Syntax

test cable-diagnostics tdr interface *interface-id*

Parameters

interface-id—(Optional) 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 1 - Test the copper cables attached to port gi1/0/1 (a copper port).

```
switchxxxxxx#  test cable-diagnostics tdr interface gi1/0/1
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 gi1/0/2
Fiber ports are not supported
```

show cable-diagnostics tdr

To display information on the last Time Domain Reflectometry (TDR) test performed on all copper ports or on a specific copper port, use the **show cable-diagnostics tdr** Privileged EXEC mode command.

Syntax

show cable-diagnostics tdr *[***interface** *interface-id*]

Parameters

- **interface-id**—(Optional) Specify an Ethernet port ID.

Command Mode

Privileged 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 [meters]	Date
gi1/0/1	OK		
gi1/0/2	Short	50	13:32:00 23 July 2010
gi1/0/3	Test has not been performed		
gi1/0/4	Open	64	13:32:00 23 July 2010

show cable-diagnostics cable-length

To display the estimated copper cable length attached to all ports or to a specific port, use the **show cable-diagnostics cable-length** Privileged EXEC mode command.

Syntax

show cable-diagnostics cable-length *[***interface** *interface-id*]

Parameters

- **interface-id**—(Optional) Specify an Ethernet port ID.

Command Mode

Privileged EXEC mode

User Guidelines

The port must be active. The cable length results are not available if link is running at 100Mbps.. The cable length results provided with this command may be effected if Green Ethernet Short Reach feature is enabled on the interface

Example

The following example displays the estimated copper cable length attached to all ports.

```
switchxxxxxx#  show cable-diagnostics cable-length
```

Port	Length [meters]
----	-----------------
gi1/0/1	< 50
gi1/0/2	Copper not active
gi1/0/3	110-140

show fiber-ports optical-transceiver

To display the optical transceiver diagnostics, use the **show fiber-ports optical-transceiver** Privileged EXEC mode command.

Syntax

show fiber-ports optical-transceiver *[***interface** *interface-id*]

Parameters

- **interface-id**—(Optional) Specify an Ethernet port ID.

Default Configuration

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

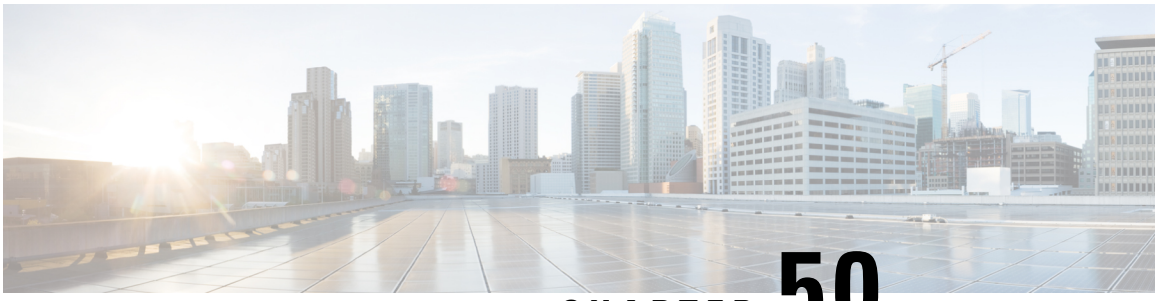
Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#  show fiber-ports optical-transceiver
   Port      Temp  Voltage Current Output  Input   LOS
             [C]   [Volt]  [mA]    Power   Power
                                   [mWatt] [mWatt]
```

```
----------- ------ ------- ------- ------- ------- ---
  gi1/0/1     Copper
  gi1/0/2     Copper
  gi1/0/3      28    3.32    7.26    3.53    3.68   No
  gi1/0/4      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
```



CHAPTER 50

PnP Commands

This chapter contains the following sections:

- pnp device, on page 811
- pnp discovery timeout, on page 812
- pnp enable, on page 813
- pnp reconnect interval, on page 813
- pnp resume, on page 814
- pnp transport, on page 814
- pnp watchdog timeout, on page 815
- show pnp, on page 816

pnp device

To define the device username and the password, use the **pnp device** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

pnp device username *username* **password** *password*

encrypted pnp device username *username* **password** encrypted-*password*

no pnp device

Parameters

- ***username***—Specifies device user name (range: 1-64 characters).
- ***password***—Specifies device password (range: 1-64 characters).
- ***encrypted-password***—Specifies encrypted device password.

Default Configuration

N/A

Command Mode

Global Configuration mode

User Guidelines

Use the **pnp device** command to configure a username and a password used in each PnP message sent by the PnP agent to a PnP server.

Example

The following example configures device name and password:

```
switchxxxxxx(config)# pnp device username sjohn password Tan123
```

pnp discovery timeout

To define the PnP agent discovery timeout in seconds and the exponential factor, use the **pnp discovery timeout** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

pnp discovery timeout *timeout exponential-factor max-timeout*

no pnp discovery timeout

Parameters

- *timeout*—Specifies the time to wait, in seconds, before attempting to discovery after a discovery is failed. The range is from 1 to 2000000.
- *exponential-factor*—Exponential factor value is the value that triggers the discovery attempt exponentially. The range is from 1 to 9.
- *max-timeout*—Specifies the maximum value of the timeout. The range is from 1 to 2000000.

Default Configuration

timeout—60 seconds

exponential-factor—3

max-timeout—540 seconds

Command Mode

Global Configuration mode

User Guidelines

Use the **pnp discovery timeout** command to configure a discovery timeout in seconds and an exponential factor. The following formula is used to calculate the next timeout using the previous one:

next-timeout = (*previous-timeout***exponential-factor* < *max-timeout*) ?

*previous-timeout*exponential-factor* : *max-timeout*;

Example

The following example configures the discovery timeout and factor:

```
switchxxxxxx(config)# pnp discovery timeout 100 2 800
```

pnp enable

To enable the PnP agent, use the **pnp enable** command in Global Configuration mode. To disable the PnP agent, use the **no** form of this command.

Syntax

pnp enable

no pnp enable

Default Configuration

PnP agent is enabled.

Command Mode

Global Configuration mode

User Guidelines

Use the command to enable the PnP agent.

Example

The following example disables the PnP agent:

```
switchxxxxxx(config)# no pnp enable
```

pnp reconnect interval

To define the PnP agent interval between sequential PnP sessions, use the **pnp reconnect interval** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

pnp reconnect interval *timeout*

no pnp reconnect interval

Parameters

- ***timeout***—Specifies the interval in seconds time before attempting to reconnect the session after a connection is lost. The range is from 1 to 2000000.The default is 30

Default Configuration

30 seconds

Command Mode

Global Configuration mode

User Guidelines

Use the **pnp reconnect interval** command to configure an interval between PnP sessions.

Example

The following example configures PnP session interval:

```
switchxxxxxx(config)# pnp interval reconnect interval 100
```

pnp resume

To resume the PnP agent, use the **pnp resume** command in Global Configuration mode.

Syntax

pnp resume

Default Configuration

PnP agent is enabled

Command Mode

Global Configuration mode

User Guidelines

Use the **pnp resume** command, to take out immediately the PnP agent from a waiting state:

- From the Discovery Waiting state to the Discovery state OR
- From the PnP Session Waiting state to the PnP Session state

Example

The following example resumes the PnP Server discovery:

```
switchxxxxxx(config)# pnp resume
```

pnp transport

To define the PnP transport, use the **pnp transport** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

pnp transport {**http** | **https**} *ip-address* [**port** *port-number*]

no pnp transport

Parameters

- **http** | **https**—Specifies the transport protocol.
- ***ip-address***—Specifies the IPv4 address or IPv6 address, or DNS name of the PnP server.
- ***port-number***—Specifies the TCP port of the PnP server. If the parameter is not defined then the following default value is applied:
  - **HTTP**—80
  - **HTTPS**—443

Default Configuration

- DHCP Option 43
- DNS:

  PnP Server IP Address—pnpserver

  Protocol—HTTP

  Port—80
- Cisco Cloud (Default):

  PnP Server IP Address—devicehelper.cisco.com

  Protocol—HTTPS

  Port—443

Command Mode

Global Configuration mode

User Guidelines

Use the **pnp transport** command to configure a transport protocol on whoich the PnP protocol is running.

Example

The following example configures the PnP transport:

```
switchxxxxxx(config)# pnp transport http 145.1.3.4
```

pnp watchdog timeout

To define the PnP agent watchdog timeout, use the **pnp watchdog timeout** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

pnp watchdog timeout *timeout*

no pnp watchdog timeout

Parameters

- ***timeout***—Specifies the time to wait a reply from a PnP or File server. The range is from 1 to 180.

Default Configuration

60 seconds

Command Mode

Global Configuration mode

User Guidelines

Use the **pnp watchdog timeout** command to configure a watchdog timeout in seconds.

Example

The following example configures the watchdog timeout:

```
switchxxxxxx(config)# pnp watchdog timeout 120
```

show pnp

To display the PnP agent information, use the **show pnp** command in Privileged EXEC mode.

Syntax

show pnp

Command Mode

Privileged EXEC mode

User Guidelines

Use the command to display information of the PnP agent.

Example 1. The following example displays PnP agent information when the PnP agent is disabled:

```
switchxxxxxx# show pnp
Administrative status: disabled
Operational status:
PnP Agent state:
Transport protocol: HTTP
Source Ip address:
TCP port: 80 (default)
Username:
Password's MD5 digest:
```

```
Discovery
  Timeout: 60 seconds (default)
  Exponential Factor: 3 (default)
  Maximum Timeout: 540 seconds
PnP Session Reconnection Interval:
  Current:
 >Default: 60 sec
  Manual Configuration:
  PnP:
PnP Watchdog Timeout: 60 seconds
```

Example 2. The following example displays PnP agent information when the PnP agent is not ready:

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: notReady (No PnP Server IP Address)
PnP Agent state:
Transport protocol: HTTP (from DHCP Option 43)
Server IP address:
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery
  Timeout: 60 seconds (default)
  Exponential Factor: 3 (default)
  Maximum Timeout: 540 seconds
PnP Session Reconnection Interval:
  Current:
 >Default: 60 sec
  Manual Configuration:
  PnP:
PnP Watchdog Timeout: 60 seconds
```

Example 3. The following example displays PnP agent information when the PnP agent is enabled in the PnP Session state:

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43)
Server IP address: 176.1.1.1 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

Example 4. The following example displays PnP agent information when the PnP agent is enabled in the PnP Session state and the PnP server was changed:

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43
Server IP address: 176.1.1.1 (from DHCP Option 43);
     Next session: 167.21.3.4 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
```

```
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

Example 5. The following example displays PnP agent information when the PnP agent is enabled in the PnP Session Waiting state:

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session Waiting
Transport protocol: HTTPS
Server IP address: 176.1.1.1
Source Ip address: 120.10.10.10
TCP port: 180
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 180 seconds (from PnP Backoff message)
Timer Remainder: 150 seconds
PnP Watchdog Timeout: 60 seconds
```

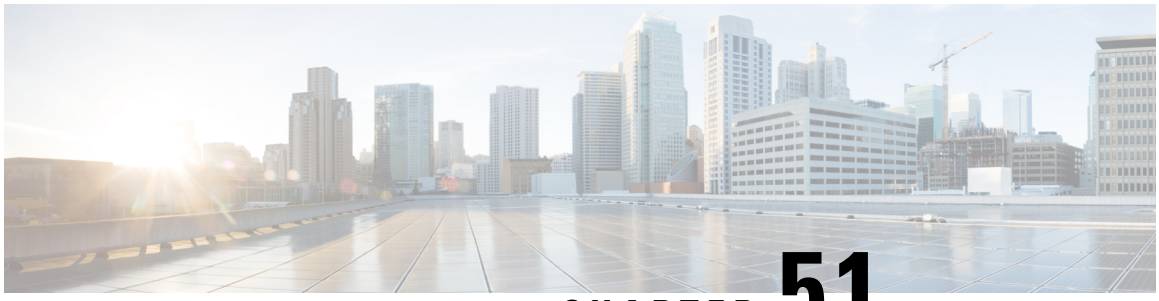
Example 6. The following example displays PnP agent information when the PnP agent is in state Discovery:

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43
Server IP address: 176.1.1.1 (from DHCP Option 43);
     Next session: 167.21.3.4 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```

Example 7. The following example displays PnP agent information when the PnP agent is in state Discovery Waiting:

```
switchxxxxxx# show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: PnP Session
Transport protocol: HTTP (from DHCP Option 43
Server IP address: 176.1.1.1 (from DHCP Option 43);
     Next session: 167.21.3.4 (from DHCP Option 43)
Source Ip address:
TCP port: 80 (default)
Username:atre1234c (from DHCP Option 43)
Password's MD5 digest: 1238af77aaca17568f1298cced165fec (from DHCP Option 43)
Discovery Timeout: 60 seconds (default)
Discovery Exponential Factor: 3 (default)
Discovery Maximum Timeout: 540 seconds
```

```
PnP Session Interval Timeout: 60 (default)
PnP Watchdog Timeout: 60 seconds
```



CHAPTER 51

PoE Commands

This chapter contains the following sections:

- power inline, on page 821
- power inline inrush test disable, on page 822
- power inline legacy support disable, on page 823
- power inline powered-device, on page 823
- power inline priority, on page 824
- power inline usage-threshold, on page 824
- power inline traps enable, on page 825
- power inline limit, on page 825
- power inline limit-mode, on page 826
- power inline negotiation, on page 827
- power inline auto-class mode, on page 827
- set power inline auto-class process, on page 828
- show power inline, on page 829
- show power inline savings, on page 833
- clear power inline counters, on page 834
- clear power inline monitor consumption, on page 835
- show power inline monitor consumption, on page 835

power inline

To configure the inline power administrative mode on an interface, use the **power inline** Interface Configuration mode command.

Syntax

power inline auto *[***time-range** *time-range-name]*

power inline never

Parameters

- **auto**—Turns on the device discovery protocol and applies power to the device.
- **never**—Turns off the device discovery protocol and stops supplying power to the device.

- **time-range-name**—Specifies a time range. When the time range is not in effect the power is not supplied the attached device. If a time range is not specified, there is no time range bounded to the port. (Range: 1–32 characters)

Default Configuration

The default configuration is set to auto.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The **never** parameter cannot be used with a time range.

Example

The following example turns on the device discovery protocol on port 4.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline auto
```

power inline inrush test disable

To disable the inrush test (a hardware test that checks input surge current for PoE devices), use the **power inline inrush test disable** Global Configuration mode command. To enable the inrush test, use the no form of this command.

Syntax

power inline inrush test disable

no power inline inrush test disable

Default Configuration

Inrush test is enabled.

Command Mode

Global Configuration mode

Example

The following example disable inrush test.

```
switchxxxxxx(config)# power inline inrush test disable
```

power inline legacy support disable

To disable the legacy PDs support, use the **power inline legacy support disable** Global Configuration mode command. To enable the legacy support, use the no form of this command.

Syntax

power inline legacy support disable

no power inline legacy support disable

Default Configuration

Legacy support is enabled.

Command Mode

Global Configuration mode

Example

The following example disables legacy PDs support.

```
switchxxxxxx(config)# power legacy support disable
```

power inline powered-device

To add a description of the device type, use the **power inline powered-device** Interface Configuration mode command. To remove the description, use the **no** form of this command.

Syntax

power inline powered-device *pd-type*

no power inline powered-device

Parameters

pd-type—Enters a comment or a description to assist in recognizing the type of the device attached to this interface. (Length: 1–24 characters)

Default Configuration

There is no description.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example adds the description ‘ip phone’ to the device connected to port 4.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline powered-device ip_phone
```

power inline priority

To configure the interface inline power management priority, use the **power inline priority** Interface Configuration (Ethernet) mode command. To restore the default configuration, use the **no** form of this command.

Syntax

power inline priority *{***critical** | **high** | **low***}*

no power inline priority

Parameters

- **critical**—Specifies that the device operation is critical.
- **high**—Specifies that the device operation is high priority.
- **low**—Specifies that the device operation is low priority.

Default Configuration

The default configuration is set to low priority.

Command Mode

Interface (Ethernet) Configuration mode

Example

The following example sets the inline power management priority of port gi1/0/4 to High.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline priority high
```

power inline usage-threshold

To configure the threshold for initiating inline power usage alarms, use the **power inline usage-threshold** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

power inline usage-threshold *percent*

no power inline usage-threshold

Parameters

percent—Specifies the threshold in percent to compare to the measured power. (Range: 1–99)

Default Configuration

The default threshold is 95 percent.

Command Mode

Global Configuration mode

Example

The following example configures the threshold for initiating inline power usage alarms to 90 percent.

```
switchxxxxxx(config)# power inline usage-threshold 90
```

power inline traps enable

To enable inline power traps, use the **power inline traps enable** Global Configuration mode command. To disable traps, use the **no** form of this command.

Syntax

power inline traps enable

no power inline traps enable

Default Configuration

Inline power traps are disabled.

Command Mode

Global Configuration mode

Example

The following example enables inline power traps.

```
switchxxxxxx(config)# power inline traps enable
```

power inline limit

To configure the power limit per port on an interface, use the **power inline limit** Interface Configuration mode command. To return to default, use the **no** form of the command.

Syntax

power inline limit *power*

no power inline limit

Parameters

power—States the port power consumption limit in Milliwatts, Range is 0-60000.

Default Configuration

The default value is 30W

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The operational power limit is the minimum of the configured power limit value and the maximum power capability on port. For example, if the configured value is higher than 15.4W on a PoE port, the operational power limit is 15.4W.

Example

The following example sets inline power on a port.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# power inline limit 2222
```

power inline limit-mode

To set the power limit mode of the system, use the **power inline limit-mode** Global Configuration mode command. To return to default, use the **no** form of this command.

Syntax

power inline limit-mode *{**class** | **port**}*

no power inline limit-mode

Parameters

- **class**—The power limit of a port is based on the class of the PD (Power Device) as detected during the classification process
- **port**—The power limit of a port is fixed regardless of the class of the discovered PD.

Default Configuration

The default value is class

Command Mode

Global Configuration mode

User Guidelines

Changing the PoE limit mode of the system will turn the power OFF and ON for all PoE ports.

Example

The following example sets the power limit to class.

```
switchxxxxxx(config)# power inline limit-mode class
"Changing the PoE limit mode of the system will turn the power OFF and ON for all PoE ports.
 Are you sure? [y/n]"
```

power inline negotiation

The power inline negotiation Interface Configuration mode command is used to select which negotiation types are allowed on an interface. To return an interface to the default supported negotiation types, use the no form of this command.

Syntax

power inline negotiation {none | all}

no power inline negotiation

Parameters

none—indicates that no negotiation is allowed on the port.

all—indicates that all supported negotiation methods are allowed on the port.

Default Configuration

All supported negotiation methods are allowed on the port.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

If the none option is selected, all negotiation packets will be ignored.

The following example disabled negotiation on a port.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# power inline negotiation none
```

power inline auto-class mode

To set the auto-class mode of an interface, use the power inline auto-class mode Interface (Ethernet) Configuration mode command. To disable auto-class mode on an interface, use the no form of this command.

Syntax

power inline auto-class mode enable

no power inline auto-class mode

Parameters

N/A

Default Configuration

Auto-class mode is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Using this command will enable auto-class mode on the interface.

If auto-class mode is enabled on an interface, and the connected PD is also enabled for auto-class, then auto-class will be activated. For a brief period, the PD will request its peak power requirement and the Switch will calculate its power class based on this peak consumption value.

In addition, when an interface is in auto-class enabled mode, auto-class can be manually activated on the interface using the command set power inline auto-class process.

Example

The following example enables auto-class on an interface.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# power inline auto-class mode enable
```

set power inline auto-class process

To initiate manual auto-class calculation on a port, use the **set power inline auto-class process** command in Privileged EXEC mode.

Syntax

set power inline auto-class process *interface-id*

Parameters

interface-id - Specifies a 802.3BT PoE Ethernet port.

Default Configuration

N/A.

User Guidelines

Using this command will trigger a manual auto-class calculation process, using the current power consumption of the port as the peak consumption value.

This command can only be used on ports whose auto-class mode is enabled (command power inline auto-class mode).

Command Mode

Privileged EXEC mode

Example

The following command manually initiates an auto-class calculation on port gi1/0/1:

```
switchxxxxxx# set power inline auto-class process gi1/0/1
```

show power inline

To display information about the inline power for all interfaces or for a specific interface, use the **show power inline** privileged EXEC mode command.

Syntax

show power inline [*interface-id* | ***module*** *unit-id*]

Parameters

- **interface-id**—Specifies an interface ID. The interface ID must be an Ethernet port.
- **module** *unit-id*—Specifies the unit ID of the stack member.

Default Configuration

Show information for all ports.

Command Mode

Privileged EXEC mode

User Guidelines

In a stack, only devices which support PoE are displayed.

Example 1—The following example displays information about the inline power for all ports (port power based).

```
switchxxxxxx(config)# show power inline
Port limit mode: Enabled
Usage threshold: 95%
Trap: Enabled
Legacy Mode: Disabled
Inrush test: Enabled
Class Error Detection: Enabled
'
```

Unit	Module	Nominal Power (w)	Allocated Power (w)	Temp (c)	SW Version	PSE chipset HW Revisi
------	----------	----------	----------	----------	----------	----------

Unit	Module	Nominal Power (w)	Allocated Power (w)	Temp (c)	SW Version	PSE chipset HW Revision
1	48P	320	120 (37.5%)	30	1.222.3	PD69208 - 0x4BC2 PD69204 - 0x4AC2
2	24P	240	0 (0%)	50	1.222.3	PD69208* - 0x4AC2
3	24P	120	0 (0%)	50	4.0.10.0	TPS3288 - 0x40c4

Interface	Admin	Oper	Power	Class	Device	Priority
--------	----------	------------	---------	-------	-------------------	-----------
gi1/0/1	Auto	On	15.4(30)	3	IP Phone Model A	Critical
gi1/0/2	Auto	Searching	0	0		High
gi1/0/3	Never	Off	0	0		Low

Example 2—The following example displays information about the inline power for a specific port.

```
switchxxxxxx(config)# show power inline gi1/0/1
```

Interface	Admin	Oper	Power	Class	Device	Priority
--------	----------	------------	---------	-------	-------------------	-----------
gi1/0/1	Auto	On		3	IP Phone Model A	Critical

```
Port status: Port is on - Valid PD resistor signature detected
Port standard: 802.3AT
Admin power limit: 30.0 watts
Time range:
Link partner standard: 802.3AF
Operational power limit: 30 watts
Negiotiated power: 18 watts (LLDP)
```

#EDITOR: Power negotiation is done via CDP/LLDP . In case there was no power negotiation with PD, the display of protocol type will be (none). In case there was power negotiation, but it did not end in allocation of power by PSE, display will be "0 watts (LLDP)" (power could still be allocated by Hardware). In case negotiation has expired, the word "Expired" will be added, with the latest value that was negotiated (e.g. "20Watts (LLDP - Expired)").

```
Allocated power: 16 watts
Current (mA): 81
Voltage(V): 50.8
Overload Counter: 5
Denied Counter: 2
Absent Counter: 0
Invalid Signature Counter: 0
```

The following table describes the fields shown in the display:

Field	Description
Power	Inline power sourcing equipment operational status.

Field	Description
Nominal Power	Inline power sourcing equipment nominal power in Watts.
Allocated Power	The current total power allocation in Watts.
Usage Threshold	Usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.
Traps	Indicates if inline power traps are enabled.
Port	Ethernet port number.
device	Description of the device type.
State	Indicates if the port is enabled to provide power. The possible values are Auto or Never.
Priority	Port inline power management priority. The possible values are Critical, High or Low.
Status	Power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.
Class	Power consumption classification of the device.
Overload Counter	Counts the number of overload conditions detected.
Short Counter	Counts the number of short conditions detected.
Denied Counter	Counts the number of times power was denied.
Absent Counter	Counts the number of times power was removed because device dropout was detected.
Invalid Signature Counter	Counts the number of times an invalid signature of a device was detected.
Inrush Test	Displays whether the inrush test is enabled or disabled.

Field	Description
Port limit mode	Enabled for port limit and Disable for class limit.
Legacy Mode	Enabled of Disabled legacy device support.
Inrush Test	Displays whether the inrush test is enabled or disabled.
SW version	The POE firmware version.
HW Version	The POE hardware version
Usage Threshold	Usage threshold expressed in percent for comparing the measured power and initiating an alarm if threshold is exceeded.

Field	Description
Traps	Indicates if inline power traps are enabled.
Module	The module name.
Available Power	Inline power sourcing equipment nominal power in Watts.
Allocated Power	The current total power allocation in Watts.
Temp	Show the POE device temperature.
Interface	Ethernet port number.
Admin	Indicates if the port is enabled to provide power. The possible values are Auto or Never.
Oper	Power operational state. The possible values are On, Off, Test-Fail, Testing, Searching or Fault.
Power	Power consumed in watts, any allocated Power will appear in parens ().
Class	Power consumption classification of the device (0-4).
Device	Description of the device type set by the user.
Priority	Port inline power management priority. The possible values are Critical, High or Low.
Port status	The port status on/off with detailed reason (see bellow for details).
Port standard	802.3AF /802.3AT /60W POE.
Admin power limit	Port limit in watts used when the **Port limit mode** is Enabled.
Time Range	The name of the time range associated with the interface.
Link partner standard	802.3AF/802.3AT/60W POE.
Operational Power Limit	Port actual power limit in watts.
Current (mA)	Port current in Milli-Ampere.
Voltage (V)	Port voltage in volts.
Overload Counter	Counts the number of overload conditions detected.
Short Counter	Counts the number of short conditions detected.
Denied Counter	Counts the number of times power was denied.
Absent Counter	Counts the number of times power was removed because device dropout was detected.

Field	Description
Invalid Signature Counter	Counts the number of times an invalid signature of a device was detected.

```
Following is a list of port status values:
Port is on - Valid capacitor/resistor detected.
Port is on - Valid resistor/capacitor detected.
Port is on - 4 pairs.
Port is on - Forced 4 pairs.
Port is off - Main supply voltage is high.
Port is off - Main supply voltage is low.
Port is off - Hardware pin disables all ports.
Port is off - Non-existing port number.
Port is yet undefined.
Port is off - Internal hardware fault.
Port is off - User setting.
Port is off - Detection is in process.
Port is off - Non-802 - 3af powered device.
Port is off - Overload & Underload states.
Port is off - Underload state.
Port is off - Overload state.
Port is off - Power budget exceeded.
Port is off - Internal hardware fault.
Port is off - Voltage injection into the port.
Port is off - Improper Capacitor Detection results.
Port is off - Discharged load.
Port is on - Detection regardless (Force On).
Undefined error during Force On.
Supply voltage higher than settings.
Supply voltage lower than settings.
Disable_PDU flag raised during Force On.
Port is forced on, then disabled.
Port is off - Forced power error due to Overload.
Port is off - Out of power budget while in Force On.
Communication error with PoE devices after Force On.
Port is off - Short condition.
Port is off - Over temperature at the port.
Port is off - Device is too hot.
Unknown device port status.
ForcePowerErrorShortCircuit.
ForcePowerErrorChannelOverTemperature.
ForcePowerErrorChipOverTemperature .
PowerManagment - Static Calculated power is bigger than power limit.
PowerManagment - Static OVL PD class report (user predefined power value).
Static Calculated power (power limit during Force On).
Static OVL PD class report (user predefined power value during Force On).
High power port is ON - High power device was detected.
Chip Over Power - Sum of square currents exceeded SumPowerLimit.
Force Power Error Chip Over Power, during Force On.
Port is off - Class Error - Illegal class.
```

show power inline savings

To display information about the device inline power saving, use the **show power inline savings** privileged EXEC mode command.

Syntax

show power inline savings

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show power inline savings** command to display the total power saved by using the PoE time range feature which shuts down PoE to ports in specific times.

Example 1—The following example displays PoE power saving on device.

```
switchxxxxxx(config)# show power inline savings
Current Power Savings: 45W
Cumulative Energy Saved: 180 [Watt*Hour]
* Estimated Annual Power saving: 1800 [Watt*Hour]
* Annual estimate is based on the saving during the previous week
NA – information for previous week is not available
```

clear power inline counters

To clear power inline interface counters, use the **clear power inline counters** Privileged EXEC mode command.

Syntax

clear power inline counters [*interface-id*]

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID must be an Ethernet port type. If interface ID is not specified - counters for all interfaces are cleared.

Default Configuration

All interface counters are cleared.

Command Mode

Privileged EXEC mode

User Guidelines

The **clear power inline counters** command is used to reset power inline interface counters: Overload, Short, Denied, Absent and Invalid Signature .

The following example clears the power inline counters for gi1/0/2.

```
switchxxxxxx#  clear power inline counters gi1/0/2
```

clear power inline monitor consumption

To clear power inline consumption monitor info on all or on a specific interface or interface list, use the **clear power inline monitor consumption** Privileged EXEC mode command.

Syntax

clear power inline monitor consumption *[interface-id-list]*

Parameters

interface-id-list—(Optional) Specifies a list of interface ID. The interface ID must be an Ethernet port type. If interface ID is not specified - consumption information for all interfaces is cleared.

Default Configuration

All monitored interface info are cleared.

Command Mode

Privileged EXEC mode

Example

The following example clears the monitored statistics for gi1/0/1.

```
switchxxxxxx#  clear power inline monitor consumption gi1/0/1
```

show power inline monitor consumption

To display the average monitored power consumption info, use the **show power inline monitor consumption** Privileged EXEC mode command

Syntax

show power inline monitor consumption {**interface** *interface-id* | **Unit** *unit-id***}** {**minutes**|**hours | days |weeks**}

Parameters

- **interface** *interface-id*— Specifies an interface ID. The interface ID must be an Ethernet port.
- **Unit** *unit-id* - Total PoE consumption info for specified unit ID will be displayed
- **minutes** —Average minute consumption. Displays the last 60 samples, sampled every 60 seconds (every round minute according to system time)
- **hours** —Average hour consumption. Displays the last 24 samples, sampled every 60 minutes (every round hour according to system time).
- **days** —Average daily consumption. Displays the last 7 samples, sampled every 24 hours (midnight to midnight according to system time).

- **weeks** —Average Weekly Consumption. Displays the last 52 samples, sampled every 7 days (midnight Saturday to midnight Saturday according to system time).

Default Configuration

This command has no default settings.

Command Mode

Privileged EXEC mode

User Guidelines

The **show power inline monitor** is used to show average power consumption for specified time frame.

Note: only **days** and **weeks** samples are persisted after reload.

Example 1:

The following example displays the average hourly power consumption for the past day gathered for interface gi1/0/1.

```
switchxxxxxx#  show power inline monitor consumption gi1/0/1 hours
```

Sample Time	Consumption (W)
03:00:00	7.1
02:00:00	7.1
01:00:00(~)	8.5
00:00:00	9.0

(~) Not all samples are available.

* time stamp represents end of sampling period

Example 2:

The following example displays the average weekly power consumption for the past 52 weeks gathered for unit 1 .

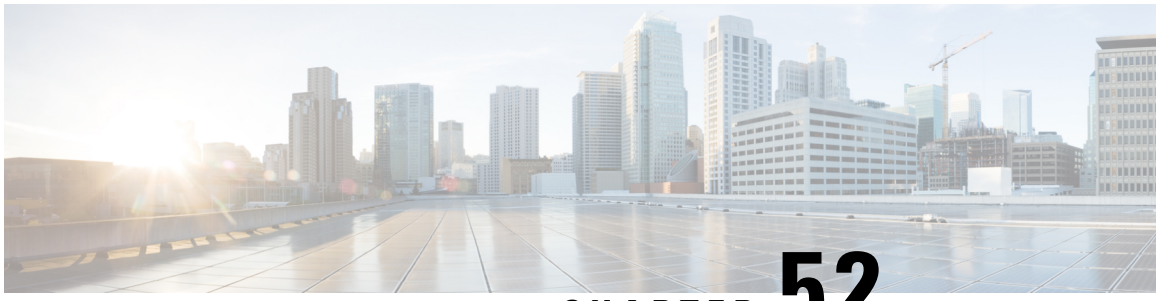
```
switchxxxxxx#  show power inline monitor  consumption  unit 1  weeks
```

Sample Time	Consumption (W)
Sun 15/11/2015 00:00:00	55.1
Sun 22/11/2015 00:00:00	75.2
Sun 29/11/2015 00:00:00(~)	45.3

```
 unit 1
```

(~) Not all samples are available.

* time stamp represents end of sampling period



CHAPTER 52

Port Channel Commands

This chapter contains the following sections:

- channel-group, on page 837
- port-channel load-balance , on page 838
- show interfaces port-channel, on page 838

channel-group

To associate a port with a port-channel, use the **channel-group** Interface (Ethernet) Configuration mode command. To remove a port from a port-channel, use the **no** form of this command.

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 (Ethernet) Configuration mode

Default mode is **on**.

User Guidelines

LACP starts to manage port joining.

When the **auto** mode is configured and there are not received LACP messages on all port-candidates then one of candidates is joined. When the first LACP message is received the port is disjoined and LACP starts to manage port joining.

Example

The following example forces port gi1/0/1 to join port-channel 1 without an LACP operation.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  channel-group 1 mode on
```

port-channel load-balance

To configure the load balancing policy of the port channeling, use the **port-channel load-balance** Global Configuration mode command. To reset to default, use the **no** form of this command.

Syntax

port-channel load-balance *{***src-dst-mac** | **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.

Default Configuration

src-dst-mac

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)#  port-channel load-balance src-dst-mac
```

show interfaces port-channel

To display port-channel information for all port channels or for a specific port channel, use the **show interfaces port-channel** Privileged EXEC mode command.

Syntax

show interfaces port-channel *[interface-id]*

Parameters

interface-id—(Optional) Specify an interface ID. The interface ID must be a port channel.

Command Mode

Privileged 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: 1,Inactive: gi1/0/2-3
Po2      Active: 5 Inactive: gi1/0/4
```



CHAPTER 53

QoS Commands

This chapter contains the following sections:

- qos, on page 842
- qos advanced-mode trust, on page 843
- show qos, on page 843
- class-map, on page 844
- show class-map, on page 845
- match, on page 846
- policy-map, on page 846
- class, on page 847
- show policy-map, on page 848
- trust, on page 849
- set, on page 849
- redirect, on page 850
- mirror, on page 851
- police, on page 852
- service-policy, on page 853
- qos aggregate-policer, on page 855
- show qos aggregate-policer, on page 856
- police aggregate, on page 857
- wrr-queue cos-map, on page 858
- wrr-queue bandwidth, on page 859
- priority-queue out num-of-queues, on page 859
- traffic-shape, on page 860
- traffic-shape queue, on page 861
- qos wrr-queue wrtd, on page 862
- show qos wrr-queue wrtd, on page 862
- show qos interface, on page 863
- qos map policed-dscp, on page 865
- qos map dscp-queue, on page 866
- qos trust (Global), on page 866
- qos trust (Interface), on page 867
- qos cos, on page 868
- qos dscp-mutation, on page 868

- show qos map, on page 869
- clear qos statistics, on page 870
- qos statistics policer, on page 871
- qos statistics aggregate-policer, on page 871
- clear queue statistics, on page 872
- show queue statistics, on page 872
- show qos statistics, on page 874

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, on page 843 command to specify the trust mode.

Default Configuration

QoS basic mode

Command Mode

Global Configuration mode

Example 1—The following example disables QoS on the device.

```
switchxxxxxx(config)#  no qos
```

Example 2—The following example enables QoS advanced mode on the device with the **ports-not-trusted** option.

```
switchxxxxxx(config)# qos advanced
```

qos advanced-mode trust

Use the **qos advanced-mode trust** Global Configuration mode 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 mode

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 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
```

show qos

Use the **show qos** Privileged EXEC mode command to display the QoS information for the device. The trust mode is displayed for the QoS basic mode.

Syntax

show qos

Default Configuration

Disabled Command Mode

Command Mode

Privileged EXEC mode

User Guidelines

Trust mode is displayed if QoS is enabled in basic mode.

Examples

```
switchxxxxxx(config)# show qos
Qos: Disabled
switchxxxxxx(config)# show qos
Qos: Basic mode
Basic trust: dscp
switchxxxxxx(config)# show qos
Qos: Advanced mode
Advanced mode trust type: cos
Advanced mode ports state: Trusted
```

class-map

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.

Syntax

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name*

Parameters

- ***class-map-name***—Specifies the class map name. (Length: 1–32 characters)
- **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. If neither **match-all** nor **match-any** is specified, the **match-all** parameter is selected by default.
- **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

No class map.

Command Mode

Global Configuration mode

User Guidelines

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. It defines a traffic flow by determining which packets match some or all of the criteria specified in the ACLs.

All class map commands are only available when QoS is in advanced mode.

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 a few **match** commands, each must point to a different type of ACL, such as: one IP ACL, one IPv6 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, on page 846 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, on page 846: 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
```

show class-map

The **show class-map** Privileged EXEC mode 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. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

Example

The following example displays the class map for Class1.

```
switchxxxxxx(config)# show class-map
Class Map matchAny class1
   Match access-group mac
```

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.

Syntax

match access-group *acl-name*

no match access-group *acl-name*

Parameters

acl-name—Specifies the MAC, IP ACL name, or IPv6 ACL name. (Length: 1–32 characters)

Default Configuration

No match criterion is supported.

User Guidelines

This command is available only when the device is in QoS advanced mode.

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
```

policy-map

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.

Syntax

policy-map *policy-map-name*

no policy-map *policy-map-name*

Parameters

policy-map-name—Specifies the policy map name. (Length: 1–32 characters)

Command Mode

Global Configuration mode

User Guidelines

This command is only available when QoS is in advanced mode.

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. 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. 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.

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)#
```

class

Use the **class** Policy-map Configuration mode. command after the policy-map, on page 846 command to attach ACLs to a policy-map. Use the **no** form of this command to detach a class map from a policy map.

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. (Length: 1–32 characters)
- **access-group** *acl-name*—Specifies the name of an IP, IPv6, or MAC Access Control List (ACL). (Length: 1–32 characters)

Default Configuration

No class map is defined for the policy map.

Command Mode

Policy-map Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

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, on page 853 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
```

show policy-map

Use the **show policy-map** Privileged 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. (Length: 1–32 characters)

Default Configuration

All policy-maps are displayed.

Command Mode

Privileged EXEC mode

Example

The following example displays all policy maps.

```
switchxxxxxx(config)#   show policy-map
Policy Map policy1
class class1
set dscp 7
Policy Map policy2
class class 2
police 96000 4800 exceed-action drop
class class2
redirect gi1/0/2
class class 3
```

```
police 96000 4800 exceed-action policed-dscp-transmit peak 128000 9600 violate-action
policed-dscp-transmit
```

trust

Use the **trust** Policy-map Class Configuration mode. command to configure the trust state. Use the **no** form of this command to return to the default trust state.

Syntax

trust

no trust

Default Configuration

The default state is according to the mode selected in the command (advanced mode). The type of trust is determined in .

Command Mode

Policy-map Class Configuration mode.

User Guidelines

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 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.

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.

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)#  permit ip any any
switchxxxxxx(config-ip-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
```

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.

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

This command is only available when QoS is in advanced mode.

The set, on page 849 and trust, on page 849 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.

The **queue** keyword is not supported into egress policies.

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-ip-al)# permit ip any any
switchxxxxxx(config-ip-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
```

redirect

Use the **redirect** Policy-map Class Configuration mode. command to redirect a traffic flow to a given Ethernet port or port channel.

Syntax

redirect *interface-id*

no redirect

Parameters

- ***interface-id***—Specifies an Ethernet port or port channel to which the flow is redirected.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

Use the **redirect** command to redirect a frame into the VLAN the frame was assigned to.

This command is only available when QoS is in advanced mode.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and redirects the flow to Ethernet port gi1/0/2:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-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)# redirect gi1/0/2
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)#
```

mirror

Use the **mirror** Policy-map Class Configuration mode. command to mirror a traffic flow to an analyzer Ethernet port.

Syntax

mirror *session_number*

no mirror

Parameters

- *session_number*—Specify the session number identified with the SPAN or RSPAN session. Only a value of 1 is allowed.

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is only available when QoS is in advanced mode.

A frame is mirrored in the same format if it matches to one of the class ACLs regardless the command of this ACL: permit or deny.

Only one source session from VLAN and flow mirroring is supported.

Example

The following example creates an ACL, places it into a class map, places the class map into a policy map and mirrors the flow to an analyzer Ethernet port defined by session 2:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-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)# mirror 2
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
switchxxxxxx(config)#
```

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). Use the **no** form of this command to remove a policer.

Syntax

police *committed-rate-kbps committed-burst-byte* [**exceed-action** *action*] [**peak** *peak-rate-kbps peak-burst-byte* [**violate-action** *action*]]

no police

Parameters

- ***committed-rate-kbps***—Specifies the average traffic rate (CIR) in kbits per second (bps).(Range: 3–maximal port speed)
- ***committed-burst-byte***—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action**—Specifies the action taken when the committed rate is exceeded and the peak rate is not exceeded. If the keyword is not configured then the following action is applied:

  drop, if **peak** the keyword is not configured.

  policed-dscp-transmit, if **peak** the keyword is configured.
- **peak**—Specifies the Two-rate Three-color policer. If the peak rate is exceeded the packet is dropped.
- ***peak-rate-kbps***—Specifies the average traffic rate (CIR) in kbits per second (bps).(Range: 3–maximal port speed)
- ***peak-burst-byte***—Specifies the peak burst size (PBS) in bytes. (Range: 3000–19173960)

- **violate-action**—Specifies the action taken when the peak rate is exceeded. If the keyword is not configured then the **drop** action is applied.
- *action*—Specifies the taken action. The possible values are:

  drop—Drops the packet.

  policed-dscp-transmit—Remarks the packet DSCP of IP traffic. The DSCP remarking is configured by the **qos map policed-dscp** command with the **violation** keyword for the violation action and without this keyword for the exceed action. DSCP remarking will have effect only if the mode is trust dscp.

Default Usage

No policer

Command Mode

Policy-map Class Configuration mode.

User Guidelines

This command is used after the policy-map, on page 846 and class, on page 847 commands.

This command is only available when QoS is in advanced mode.

Policing uses a token bucket algorithm.

Example 1. 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 cls1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action drop
```

Example 2. The following example defines a Two-rate Three-color policer for classified traffic. When the committed traffic rate exceeds 124,000 kbps and the committed burst size exceeds 9600 bytes, the packet is marked. When the peak traffic rate exceeds 200,000 kbps and the peak burst size exceeds 19200 bytes, the packet is marked. The class is called class1 and is in a policy map called policy1.

```
switchxxxxxx(config)# policy-map policy1
switchxxxxxx(config-pmap)# class cls1
switchxxxxxx(config-pmap-c)# police 124000 9600 exceed-action policed-dscp-transmit peak
200000 19200 violate-action policed-dscp-transmi
```

service-policy

Use the **service-policy** Interface (Ethernet, Port Channel) Configuration mode mode command to bind a policy map to an interface. Use the **no** form of this command to detach a policy map from an interface.

Syntax

service-policy {**input** | **output**} *policy-map-name* [**default-action** {**permit-any** | **deny-any**}]

no service-policy input | **output**

service-policy {**input** | **output**} *policy-map-name*

Parameters

- **input**—Specifies an ingress policy.
- **output**—Specifies an egress policy.
- ***policy-map-name***—Specifies the policy map name to apply to the input interface. (Length: 1–32 characters)
- **default-action**—Specifies the default action. If the keyword is not configured then the **deny-any** default action is applied.
- **deny-any**—Deny all the packets (which were ingress of the port) that do not meet the rules in a policy.
- **permit-any**—Forward all the packets (which were ingress of the port) that do not meet the rules in a policy.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Default

Policy map is not bound.

User Guidelines

This command is only available in QoS advanced mode.

Only one policy map per interface per direction is supported.

The **service-policy output** command fails if the bound policy contains actions not supported by egress policies.

A policy map cannot be bound as input and output at the same time.

Example

The following example attaches a policy map called Policy1 to the input interface.

```
switchxxxxxx(config-if)# service-policy input policy1
```

The following example attaches a policy map called Policy1 to the input interface and forwards all packets that do not meet the rules of the policy.

```
switchxxxxxx(config-if)# service-policy input policy1 permit-any
```

The following example attaches a policy map called Policy2 to the output interface.

```
switchxxxxxx(config-if)# service-policy output policy2
```

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.

Syntax

qos aggregate-policer *aggregate-policer-name committed-rate-kbps committed-burst-byte* [**exceed-action** *action*] [**peak** *peak-rate-kbps peak-burst-byte* [**violate-action** *action*]]

no qos aggregate-policer *aggregate-policer-name*

Parameters

- ***aggregate-policer-name***—Specifies the aggregate policer name. (Length: 1–32 characters)
- ***committed-rate-kbps***—Specifies the average traffic rate (CIR) in kbits per second (bps).(Range: 3–57982058)
- ***committed-burst-byte***—Specifies the normal burst size (CBS) in bytes. (Range: 3000–19173960)
- **exceed-action**—Specifies the action taken when the committed rate is exceeded and the peak rate is not exceeded. If the keyword is not configured then the following action is applied:

  drop, if **peak** the keyword is not configured.

  policed-dscp-transmit, if **peak** the keyword is configured.
- **peak**—Specifies the Two-rate Three-color policer. If the peak rate is exceeded the packet is dropped.
- ***peak-rate-kbps***—Specifies the average traffic rate (CIR) in kbits per second (bps).(Range: 3–57982058)
- ***peak-burst-byte***—Specifies the peak burst size (PBS) in bytes. (Range: 3000–19173960)
- **violate-action**—Specifies the action taken when the peak rate is exceeded. If the keyword is not configured then the **drop** action is applied.
- ***action***—Specifies the taken action. The possible values are:
  - **drop**—Drops the packet.
  - **policed-dscp-transmit**—Remarks the packet DSCP of IP traffic. The DSCP remarking is configured by the **qos map policed-dscp** command with the **violation** keyword for the violation action and without this keyword for the exceed action. DSCP remarking will have effect only if the mode is trust dscp.

Default Configuration

No aggregate policer is defined.

Command Mode

Global Configuration mode

User Guidelines

This command is only available when QoS is in advanced mode.

Use the **qos aggregate-policer** command to define a policer that 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 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 1. 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
```

Example 2. The following example defines the parameters of a Two-rate Three-color policer called policer2 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 remarked. When the average traffic rate exceeds 200,000 kbps or the normal burst size exceeds 9600 bytes, the packet is dropped.

```
switchxxxxxx(config)# qos aggregate-policer policer2 124000 9600 exceed-action
policed-dscp-transmit peak 200000 19200 violate-action policed-dscp-transmit
```

show qos aggregate-policer

Use the **show qos aggregate-policer** Privileged EXEC mode 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. (Length: 1–32 characters)

Default Configuration

All policers are displayed.

Command Mode

Privileged EXEC mode

Example 1. 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.

Example 2. The following example displays the parameters of the aggregate Two-rate Three-color policer called Policer1.

```
switchxxxxxx# show qos aggregate-policer policer1
aggregate-policer policer1 124000 9600 exceed-action policed-dscp-transmit peak 200000 19200
 violate-action policed-dscp-transmit
```

not used by any policy map.

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. (Length: 1–32 characters)

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
```

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 1.

CoS value 1 is mapped to queue 2.

CoS value 2 is mapped to queue 3.

CoS value 3 is mapped to queue 6.

CoS value 4 is mapped to queue 5.

CoS value 5 is mapped to queue 8.

CoS value 6 is mapped to queue 8

CoS value 7 is mapped to queue 7

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
```

wrr-queue bandwidth

Use the **wrr-queue bandwidth** Global Configuration mode 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.

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.

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, on page 859 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
```

priority-queue out num-of-queues

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 the queues are expedited (strict priority queues).

Default Configuration

All queues are expedite queues.

Command Mode

Global Configuration mode

User Guidelines

An expedite queue is a strict priority queue, which is serviced until empty before the other lower priority queues are serviced.

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
```

traffic-shape

Use the **traffic-shape** Interface (Ethernet, Port Channel) 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: GE: 64kbps–maximum port speed ,10GE: 64Kbps–maximum port speed))
- **committed-burst**—Specifies the maximum permitted excess burst size (CBS) in bytes. (Range: 4096 - 16670940 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The egress port shaper controls the traffic transmit rate (Tx rate) on a port.

Example

The following example sets a traffic shaper on gi1/0/1 when the average traffic rate exceeds 64 kbps or the normal burst size exceeds 4096 bytes.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#  traffic-shape 64 4096
```

traffic-shape queue

Use the **traffic-shape queue** Interface (Ethernet, Port Channel) 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 - 16670940 bytes)

Default Configuration

The shaper is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The egress port shaper controls the traffic transmit rate (Tx rate) on a queue on a port.

Example

The following example sets a shaper on queue 1 on gi1/0/1 when the average traffic rate exceeds 124000 kbps or the normal burst size exceeds 9600 bytes.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#  traffic-shape queue 1 64 4096
```

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

Default

Disabled

Command Mode

Global Configuration mode

User Guidelines

The command is effective after reset.

Example

```
switchxxxxxx(config)# qos wrr-queue wrtd
This setting will take effect only after copying running configuration to startu
p configuration and resetting the device
switchxxxxxx(config)#
```

show qos wrr-queue wrtd

Use the **show qos wrr-queue wrtd** Privileged EXEC mode command to display the Weighted Random Tail Drop (WRTD) configuration.

Syntax

show qos wrr-queue wrtd

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx(config)# show qos wrr-queue wrtd
 Weighted Random Tail Drop is disabled
 Weighted Random Tail Drop will be enabled after reset
```

show qos interface

Use the **show qos interface** Privileged EXEC mode command to display Quality of Service (QoS) information on the interface.

Syntax

show qos interface [**buffers** | **queueing** | **policers** | **shapers**] [*interface-id*]

Parameters

- **buffers**—Displays the buffer settings for the interface's queues. For GE ports, displays the queue depth for each of the queues.
- **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.
- ***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

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.

In case of Policers, Shapers and Rate Limit - only the ports which are not in the default configuration will be showed.

Example 1—The following is an example of the output from the **show qos interface** command.

```
switchxxxxxx(config)# show qos interface gi1/0/1
Ethernet gi1/0/0/1
Default CoS: 0
Trust mode: disabled
Ingress Policy applied: AV1
Egress Policy applied: AV2
```

```
Default ACE ingress action: deny-all
Default ACE egress action: deny-all
```

Example 2—The following is an example of the output from the **show qos interface queueing** command for 4 queues.

```
switchxxxxxx(config)# show qos interface queueing gi1/0/1
Ethernet gi1/0/0/1
wrr bandwidth weights and EF priority:
qid-weights      Ef - Priority
1 - N/A          ena- 1
2 - N/A          ena- 2
3 - N/A          ena- 3
4 - N/A          ena- 4
Cos-queue map:
cos-qid
0 - 1
1 - 1
2 - 2
3 - 3
4 - 3
5 - 4
6 - 4
7 - 4
```

Example 3 —The following an example of the output from the **show qos interface buffers** command for 8 queues.

```
switchxxxxxx(config)# show qos interface buffers gi1/0/1
gi1/0/1
Notify Q depth:
buffers gi1/0/1
Ethernet gi1/0/1
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 4—This is an example of the output from the **show qos interface shapers** command.f

```
switchxxxxxx(config)# show qos interface shapers gi1/0/1
gi1/0/1
Port shaper: enable
Committed rate: 64 kbps
Committed burst: 9600 bytes
```

QID	Status	Target	Target
1	Enable	Committed	Committed
2	Disable	Rate [kbps]	Burst [bytes]
3	Enable	64	17000
4	Disable	N/A	N/A
5	Disable	N/A	N/A
6	Disable	N/A	N/A
7	Enable	N/A	N/A
8	Enable	N/A	N/A
		N/A	N/A
		N/A	N/A

Example 5—This is an example of the output from **show qos interface policer**

```
switchxxxxxx(config)#   show qos interface policer gi1/0/1
Ethernet gi1/0/1
Ingress Policers:
Class map: A
Policer type: aggregate
Commited rate: 19 kbps
Commited burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Class map: B
Policer type: single
Commited rate: 19 kbps
Commited burst: 9600 bytes
Peak rate: 26 kbps
Peak burst: 9600 bytes
Exceed-action: policed-dscp-transmit
Violate-action: drop
Class map: C
Policer type: none
Egress Policers:
Class map: D
```

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.

Syntax

qos map policed-dscp [**violation**] *dscp-list* **to** *dscp-mark-down*

no qos map policed-dscp [**violation**] [*dscp-list*]

Parameters

- **violation**—Specifies the DSCP remapping in the violate action. If the keyword is not configured the the command specifies the DSCP remapping in the exceed action.
- ***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
```

qos map dscp-queue

Use the **qos map dscp-queue** Global Configuration mode command to configure the DSCP to queue 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	9-15	0-8	17-23	32, 41-47	25-31	33-39	16,24,48,56	None
Queue-ID	2	1	3	7	4	5	6	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
```

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**| **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.
- **cos-dscp**—Specifies that ingress packets are classified with packet DSCP values, if they are IP packets and by CoS value if non IP.

Default Configuration

dscp

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
```

qos trust (Interface)

Use the **qos trust** Interface (Ethernet, Port Channel) Configuration 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

Default Configuration

Each port is enabled while the system is in basic mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures gi1/0/1 to the default trust state.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)# qos trust
```

qos cos

Use the **qos cos** Interface (Ethernet, Port Channel) Configuration 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 (Ethernet, Port Channel) Configuration 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 gi1/0/1 default CoS value as 3.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)#  qos cos 3
```

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

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
```

show qos map

Use the **show qos map** Privileged EXEC mode command to display the various types of QoS mapping.

Syntax

show qos map [dscp-queue | **dscp-dp| dscp-mutation** | policed-dscp | policed-cos]

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

Privileged EXEC mode

Example 1. The following example displays the QoS mapping information:

```
switchxxxxxx(config)# show qos map dscp-queue
Dscp-queue map:
     d1 : d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------
      0 :   01 01 01 01 01 01 01 01 01 01
      1 :   01 01 01 01 01 01 02 02 02 02
      2 :   02 02 02 02 02 02 02 02 02 02
      3 :   02 02 03 03 03 03 03 03 03 03
      4 :   03 03 03 03 03 03 03 03 04 04
      5 :   04 04 04 04 04 04 04 04 04 04
      6 :   04 04 04 04
```

Example 2. The following example displays the dscp remapping information:

```
switchxxxxxx(config)# show qos map policed-dscp
Policed-dscp map (exceed):
     d1 : d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------
      0 :   00 01 02 03 04 05 06 07 08 09
      1 :   10 11 12 13 14 15 16 17 18 19
      2 :   20 21 22 23 24 25 26 27 28 29
      3 :   30 31 32 33 34 35 36 37 38 39
      4 :   40 41 42 43 44 45 46 47 48 49
      5 :   50 51 52 53 54 55 56 57 58 59
      6 :   21  21 21
Policed-dscp map (violate):
     d1 : d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------
      0 :   00 01 02 03 04 05 06 07 08 09
      1 :   10 11 12 13 14 15 16 17 18 19
      2 :   20 21 22 23 24 25 26 27 28 29
      3 :   30 31 32 33 34 35 36 37 38 39
      4 :   40 41 42 43 44 45 46 47 48 49
      5 :   50 51 52 53 54 55 56 57 58 59
      6 :   11  11 11
```

clear qos statistics

Use the **clear qos statistics** Privileged EXEC mode command to clear the QoS statistics counters.

Syntax

clear qos statistics

Command Mode

Privileged EXEC mode

Example

The following example clears the QoS statistics counters.

```
switchxxxxxx(config)#  clear qos statistics
```

qos statistics policer

Use the **qos statistics policer** Interface (Ethernet, Port Channel) Configuration mode 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. (Length: 1–32 characters)
- **class-map-name**—Specifies the class map name. (Length: 1–32 characters)

Default Configuration

Counting in-profile and out-of-profile is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example enables counting in-profile and out-of-profile on the interface.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# qos statistics policer policy1 class1
```

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. (Length: 1–32 characters)

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
```

clear queue statistics

Use the **clear queue statistics** Privileged EXEC mode command to clear the queue statistics.

Syntax

clear queue statistics [*interface-id*]

Parameters

- ***interface-id***—Specifies an Ethernet port which queue statistics are cleared.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **clear queue statistics** *interface-id* command to clear the queue statistics of the given port.

Use the **clear queue statistics** command to clear the queue statistics of all ports.

Example

The following example clears queue statistics of Ethernet port gi1/0/2:

```
switchxxxxxx# clear queue statistics gi1/0/2
```

show queue statistics

Use the **show queue statistics** Privileged EXEC mode command to display the queue statistics.

Syntax

show queue statistics [*interface-id*] [**detailed**]

Parameters

- ***interface-id***—Specifies an Ethernet port which queue statistics are displayed.
- ***detailed*** (optional) - Displays information for all interfaces and queues. If the detailed option is not specified, then the command output will include only interfaces and queues for which the values of one of the displayed counters is non-zero

Default Configuration

By default the command will display information only for the ports and queues for which one of the displayed counters is non-zero.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show queue statistics** *interface-id* command to display the queue statistics of the given port. If the detailed option is not specified, then the command output will include only the interface queues in which the value of one of the displayed counters is non-zero.

Use the **show queue statistics detailed** command to display the statistics for all of the interfaces and queues. If the detailed option is not specified, then the command output will include only interfaces and queues for which the values of one of the displayed counters is non-zero.

Example

Example 1 -

The following example displays queue statistics for queues of Ethernet port gi1/0/2 that have non-zero value in one of the displayed counters:

```
switchxxxxxx# show queue statistics gi1/0/2
```

Interface	Queue	Tx Pkts	Tx Bytes	Tail Dropped Pkts	Tail Dropped Bytes
gi1/0/2	1	2700221	0	0	0
gi1/0/2	4	1850	257369	44543278	0
gi1/0/2	5	233017	50313150	0	10234
gi1/0/2	8	50	25600	12	0
				0	

Example 2 - The following example displays queue statistics for all queues of Ethernet port gi1/0/2:

Interface	Queue	Tx Pkts	Tx Bytes	Tail Dropped Pkts	Tail Dropped Bytes
---	---	---	---	---	---
gi1/0/2	1	2700221	0	0	0
gi1/0/2	2	0	0	44543278	0
gi1/0/2	3	0	0	0	0
gi1/0/2	4	1850	257369	0	10234
gi1/0/2	5	233017	50313150	0	0
gi1/0/2	6	0	0	12	0
gi1/0/2	7	0	0	0	0
gi1/0/2	8	0	0	0	
				0	

show qos statistics

Use the **show qos statistics** Privileged EXEC mode command to display Quality of Service statistical information.

Syntax

show qos statistics

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show qos statistics** command to display QoS statistics.

Up to 16 sets of counters can be enabled for policers. The counters can be enabled in the creation of the policers.

Example

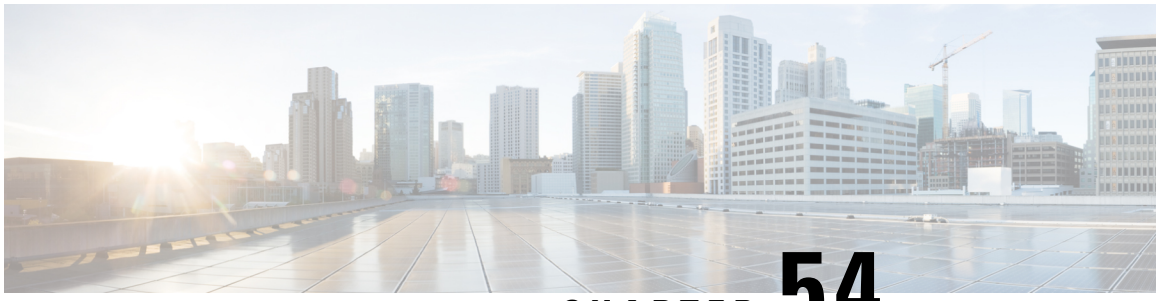
The following example displays Quality of Service statistical information.

```
switchxxxxxx# show qos statistics
Policers
---------
```

Interface	Policy Map	Class Map	In-Profile Bytes	Peak Bytes	Violate Bytes
gi1/0/1	Policy1	Class1	756457	5427	12
gi1/0/1	Policy1	Class2	8759	14	12
gi1/0/2	Policy1	Class1	75457	5	2
gi1/0/2	Policy1	Class2	5326		12

```
Aggregate Policers
```

Name	In-Profile Bytes	Peak Bytes	Violate Bytes
Policer	756457	5427	12



CHAPTER 54

RADIUS Commands

This chapter contains the following sections:

- radius-server force-message authenicator host, on page 877
- radius-server host, on page 878
- radius-server key, on page 880
- radius-server retransmit, on page 880
- radius-server host source-interface, on page 881
- radius-server host source-interface-ipv6, on page 882
- radius-server timeout, on page 883
- radius-server deadtime, on page 883
- show radius-servers, on page 884
- show radius-servers key, on page 884

radius-server force-message authenicator host



Note The radius-server force-message authenticator host command is support on firmware version 4.1.6.53 and above.

Use the radius-server force-message-authenticator Global Configuration mode command to enable Message-Authenticator attribute verification for all types of RADIUS responses received from the specified RADIUS server. Use the no form of the command to restore the default setting.

Syntax

radius-server force-message-authenticator host {ip-address | hostname}

no radius-server force-message-authenticator 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.
- *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)

Default Configuration

Message-Authenticator attribute verification is enabled only for RADIUS responses that are part of a RADIUS exchanges using EAP authentication.

Command Mode

Global Configuration mode

User Guidelines

Use the radius-server force-message-authenticator command to to ensure that all RADIUS responses from the specified server include the Message-Authenticator attribute (RADIUS attribute 80. If this setting is enabled, any type of RADIUS response that does not include the Message-Authenticator attribute will be silently discarded and the event will be logged. If this only if they are part of an RADIUS exchange using EAP authentication.

The command will fail if the RADIUS server specified in the host parameter was not previously configured on the device using the radius-server host command.

Examples

Example 1 - The following example enables Message-Authentication attribute verification for all types of RADIUS responses received from RADIUS server 1.2.3.4.

```
switchxxxxxx(config)# radius-server force-message-authenticator host 1.2.3.4
```

Example 2 - In the following example the attempt to enable Message-Authentication attribute verification for all types of RADIUS responses received from RADIUS server 5.6.7.8 fails because RADIUS server 5.6.7.8 is not configured on the device.

```
switchxxxxxx(config)# radius-server force-message-authenticator host 5.6.7.8
Command failed since RADIUS server 5.6.7.8 was not configured on the device.
```

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*] [**priority** *priority*] [**usage** {**login** | **dot1.x** | **all**}]

encrypted radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *encrypted-key-string*] [**priority** *priority*] [**usage** {**login** | **dot1.x** | **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.

- ***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** *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.
- **priority** *priority*—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- **usage** {**login** | **dot1.x** | **all**}—Specifies the RADIUS server usage type. The possible values are:

  login—Specifies that the RADIUS server is used for user login parameters authentication.

  dot1.x—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 the command) is used.

If **retransmit** is not specified, the global value (set in the command) is used.

If **key-string** is not specified, the global value (set in the command) is used.

If the **usage** keyword is not specified, the **all** argument is applied.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, this command is used for each host.

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
```

radius-server key

Use the **radius-server key** Global Configuration mode command to set the authentication key for RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server key [*key-string*]

encrypted radius-server key [*encrypted-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)
- ***encrypted-key-string***—Same as the key-string parameter, but the key is in encrypted form.

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

Example

The following example defines the authentication key for all RADIUS communications between the device and the RADIUS daemon.

```
switchxxxxxx(config)# radius-server key enterprise-server
```

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
```

radius-server host source-interface

Use the **radius-server host source-interface** Global Configuration mode command to specify the source interface whose IPv4 address will be used as the Source IPv4 address for communication with IPv4 RADIUS servers. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server host source-interface *interface-id*

no radius-server host source-interface

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 RADIUS server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface vlan 100
```

radius-server host source-interface-ipv6

Use the **radius-server host source-interface-ipv6** Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 RADIUS servers. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server host source-interface-ipv6 *interface-id*

no radius-server host source-interface-ipv6

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 RADIUS server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface-ipv6 vlan 100
```

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
```

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
```

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
IP address  Port Port Time                Dead    Deadtime
            Auth Acc  Out   Retransmission time    status     Priority Usage
----------  ---- ---- ----  ------------- ------    ------    -------- -----
172.16.1.1  1812 1813  125  Global        Global     Dead        1      All
172.16.1.2  1812 1813  102  8             Global      Up         2      All
Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

show radius-servers key

Use the **show radius-servers key** Privileged EXEC mode command to display the RADIUS server key settings.

Syntax

show radius-servers key

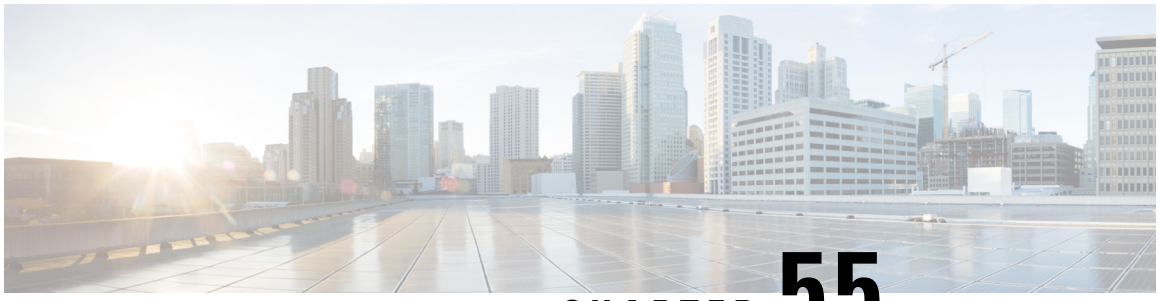
Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server key settings.

```
switchxxxxxx# show radius-servers key

IP address                     Key (Encrypted)
----------                     ---------------
172.16.1.1                     1238af77aaca17568f1298cced165fec
172.16.1.2                     1238af77aaca17568f12988601fcabed

Global key (Encrypted)
----------------------
1238af77aaca17568f1298bc5476ddad
```



CHAPTER 55

CoA Commands

This chapter contains the following sections:

- aaa server radius dynamic-author, on page 887
- attribute event-timestamp drop-packet, on page 888
- authentication command bounce-port ignore, on page 889
- authentication command disable-port ignore, on page 889
- client, on page 890
- domain delimiter, on page 891
- domain stripping, on page 892
- ignore server-key, on page 893
- port, on page 894
- server-key, on page 895
- show aaa clients, on page 895
- clear aaa counters clients, on page 897
- show aaa server radius dynamic-author, on page 897

aaa server radius dynamic-author

Use the aaa server radius dynamic-author global configuration mode command to enter into the dynamic authorization local server configuration mode, and configure the Change of Authorization (CoA) clients and parameters.

Syntax

aaa server radius dynamic-author

Parameters

This command has no arguments or keywords.

Command Mode

Global configuration mode

User Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to the device via PoD (Packet of Disconnect) or CoA (Change of Authorization) Requests. This command enters the dynamic authorization local server configuration mode. Once in this mode, Dynamic RADIUS related commands (like client address or key) can be configured.

Examples

The following example enters the dynamic authorization local server configuration mode context:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)#
```

attribute event-timestamp drop-packet

To configure the device to discard a Packet of Disconnect (POD) Request or Change of Authorization (CoA) Request that do not include an Event-Timestamp Attribute use the attribute event-timestamp drop-packet command in dynamic authorization local server configuration mode. To restore the default configuration, use the no form of this command.

Syntax

attribute event-timestamp drop-packet

no attribute event-timestamp drop-packet

Parameters

This command does not have any parameters.

Default Configuration

The device does not discard PoD or CoA requests even if they do not contain the event-timestamp attribute.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

The Event-Timestamp (RADIUS attribute 55 - [RFC2869]) is used by the Switch to check if the Requests are current. If requests are not current, they are silently discarded (RFC 5176). It is not mandatory for CoA clients to send this attribute. To enhance CoA security, use the attribute event-timestamp drop-packet command to discard PoD or CoA requests that do not include the Event-Timestamp RADIUS attribute.

Examples

In the following example the device is configured to discard PoD or CoA Requests that do not include the Event-Timestamp RADIUS attribute:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# attribute event-timestamp drop-packet
```

authentication command bounce-port ignore

To configure the device to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the authentication command bounce-port ignore command in global configuration mode. Use the no form of this command to return to the default status.

Syntax

authentication command bounce-port ignore

no authentication command bounce-port ignore

Parameters

This command has no arguments or keywords.

Default Configuration

The device accepts a RADIUS CoA bounce port command.

Command Mode

Global configuration mode

User Guidelines

which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer), that does not have a mechanism to detect a change on this authentication port. The authentication command bounce-port ignore command configures the device to ignore the RADIUS CoA bounce port command to prevent a link flap from occurring on any host(s) that are connected to an authentication port.

Examples

The following example shows how to configure the device to ignore a CoA bounce port command:

```
Switch010203(config)# authentication command bounce-port ignore
```

authentication command disable-port ignore

To configure the device to ignore a RADIUS Change of Authorization (CoA) disable-port command, use the authentication command disable-port ignore command in global configuration mode. Use the no form of this command to return to the default status.

Syntax

authentication command disable-port ignore

no authentication command bounce-port ignore

Parameters

This command has no arguments or keywords.

Default Configuration

The device accepts a RADIUS CoA disable port command.

Command Mode

Global configuration mode

User Guidelines

The RADIUS CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the authentication command disable-port ignore command to configure the device to ignore the RADIUS CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

Examples

Example 1

The following example shows how to configure the device to ignore a CoA disable port command:

```
Switch010203(config)# authentication command disable-port ignore
```

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the client command in dynamic authorization local server configuration mode. To remove a client, use the no form of this command.

Syntax

client *ip-address*s *[***server-key** *key-string*]

encrypted client *ip-address* **server-key** *encrypted-key-string*

no client *ip-address*

Parameters

- *ip-address* - Specifies the CoA client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address
- **server-key** *key-string* – (optional) - Configures the RADIUS key to be shared between the device and a CoA client (Range: 0–128 characters). To specify an empty string, enter "".
- **server-key** *encrypted-key-string* - Same as the key-string parameter, but the key is in encrypted form.

Default Configuration

CoA clients are not configured on the device.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

Use the client command to allow an external policy server (configured in this command) to dynamically send updates to the device. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling the device and an external policy server each to act as a CoA server and client. Use the client command to specify the CoA clients for which the device will act as a server.

Use the optional server-key parameter to specify the key for RADIUS communications between the device and the specified CoA client. This key must match the key used by the CoA client. To specify an empty string, enter "". If this parameter is omitted, the global CoA key (command server-key) is used. If a global key was not configured the RADIUS exchange between the device and CoA client will fail.

If the ignore server-key command is configured then the RADIUS exchange between the device and CoA client will succeed even if there is a key mismatch or if a key was not configured.

Examples

Example 1

In the following example a CoA client with IP address 1.1.1.1 is added with a server key of “key1”:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# client 1.1.1.1 server-key key1
```

Example 2

In the following example a CoA client with IP address 2.2.2.2 is added without configuring a client server-key. In this case the global server-key (if configured) is used:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# client 2.2.2.2
```

domain delimiter

To configure the username domain delimitator for received PoD and CoA Requests use the domain delimiter command in dynamic authorization local server configuration mode. To return to the default delimiter, use the no form of this command.

Syntax

domain delimiter *character*

no domain delimiter

Parameters

- delimiter character — Specifies the domain delimiter. One of the following options can be specified: @, /, $, %, \, # or -

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

Default Configuration

The default delimiter is the @ character.

User Guidelines

Use the domain delimiter command to configure the delimiter to use when stripping the full username for AAA or 802.1x user sessions, to compare to the username provided in the packet of disconnect (POD) or Change of Authorization (CoA) requests. See command domain delimiter for details of full username domain section stripping.

Examples

Example 1

In this example the $ character is configured as a delimiter:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain delimiter $
```

domain stripping

To enable and define the behavior for username domain stripping for received PoD and CoA Requests use the domain stripping command in dynamic authorization local server configuration mode. To return to the default setting, use the no form of this command.

Syntax

domain stripping [right-to-left]

no domain stripping

Parameters

stripping — Compares the incoming username with the names oriented to the left of the domain delimiter

stripping [right-to-left] (optional) - Terminates the string at the first delimiter going from right to left

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

Default Configuration

Stripping is disabled by default. Stripping default direction is left-to-right.

User Guidelines

Use the domain stripping command to enable username domain stripping based on the delimiter configured in the domain delimiter command. Domain stripping allows to compare the incoming username with the names oriented to the left of the @ domain delimiter.

Configuring domain stripping allows you to send disconnect messages with only the username present before the @ domain delimiter (or other delimiter configured using the command domain delimiter. The switch then compares and matches this username with any session username on the switch with a potential domain. For

example, when domain stripping is configured and you send packet of disconnect (POD) or Change of Authorization (CoA) Requests with the username “test,” a comparison between the PoD/CoA message and device session username takes place, and sessions with the username “test@example.com” or “test” match the specified username “test.”.

If domain stripping is not configured (the default behavior), the username provided in the PoD and COA Requests are compared with the full usernames included on the device active sessions.

Use the right-to-left keyword to specify that the username string should be terminated the string at the first delimiter going from right to left.

Examples

Example 1:

In this example the $ character is configured as a delimiter, and stripping is performed to the left of the delimiter. In this case, if the session user-name is user1$my_users then the username to be matched in the PoD or CoA Request is “user1”:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain delimiter $
Switch010203(config-locsvr-da-radius)# domain stripping
```

Example 2:

In this example stripping is performed up to the 1st delimiter to the left of the first delimiter going from right to left, using the default delimiter of @. In this case, if the session user-name is user1@test.com@example.com then the username to be matched in the PoD or CoA Request is “user1@test.com”:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# domain stripping right-to-left
```

ignore server-key

To configure the device to ignore the CoA server-key use the ignore server-key command in dynamic authorization local server configuration mode. To restore the default configuration, use the no form of this command.

Syntax

ignore server-key

no ignore server-key

Default Configuration

The server-key is not ignored.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius).

User Guidelines

Use the ignore server-key command to configure the device to ignore the server key sent in the PoD or CoA Requests. If the server-key is ignored the RADIUS exchange with the CoA client will succeed even in a CoA

server-key was not configured on the device (commands client or server-key) or if the key configured on the device does not match the key provided in the PoD or CoA Requests.

The default behavior is not to ignore the server key, meaning that PoD or CoA Requests will be discarded in case of a key mis-match or if a key was not configured for the CoA client.

Examples

Example 1:

In the following example the device is configured to ignore the server key:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# ignore server-key
```

port

To specify the port on which a device listens for Change of Authority (CoA) and Packet of Disconnect (PoD) Requests from configured CoA clients, use the port command in dynamic authorization local server configuration mode. To restore the default configuration, use the no form of this command.

Syntax

port udp-port

no port

Parameters

- *udp-port*—Specifies the UDP port number for authentication requests. (Range: 0–59,999)

Default Configuration

The device listens for CoA and PoD Requests on UDP port 1700.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

Use the port command to specify the port on which the device will listen for requests from CoA clients. This configuration applies to RADIUS PoD or CoA Requests from all CoA clients. If the port number is set to 0, PoD and CoA Requests are dropped even if CoA clients have been configured.

Examples

Example 1:

In the following example a port 1648 is specified as the port on which the device listens for RADIUS PoD and CoA requests:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# port 1648
```

server-key

To configure the default RADIUS key to be shared between the device and the CoA, use the server-key command in dynamic authorization local server configuration mode. To remove the configuration, use the no form of this command.

Syntax

server-key *key-string*

encrypted server-key *encrypted-key-string*

no server key

Parameters

- *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the CoA client's server (Range: 0–128 characters). The key provided in the PoD or CoA request must match this key. To specify an empty string, enter "".
- *encrypted-key-string*—Same as the key-string parameter, but the key is in encrypted form

Default Configuration

default server key is not configured.

Command Mode

Dynamic authorization local server configuration (config-locsvr-da-radius)

User Guidelines

Use the server-key command to define the default RADIUS key to be used in communications between the device and the CoA client. This key is used by clients that were not configured with a specific client key (command client)

This key must match the key used by the CoA client. To specify an empty string, enter "".

If the ignore server-key command is configured then the RADIUS exchange between the device and CoA client will succeed even if there is a key mismatch or if a key was not configured

Examples

Example 1:

In the following example a default server key "key123" is configured:

```
Switch010203(config)# aaa server radius dynamic-author
Switch010203(config-locsvr-da-radius)# server-key key123
```

show aaa clients

Use the show aaa clients Privilege EXEC mode command to show AAA (CoA) client's statistics.

- ip-address (optional) —Displays the statistics for a specific CoA client host. The IP address can be an IPv4, IPv6 or IPv6z address.

Default Configuration

By default, the statistics of all CoA hosts are display.

Command Mode

Privileged EXEC mode

Examples

```
Switch010203# show aaa clients

Dynamic Author Client 1.1.1.1
CoA: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
PoD: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
Average Ack response time: 0 msec

Dynamic Author Client 2.2.2.2
CoA: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
PoD: requests: 0, transactions: 0
retransmissions: 0, active transactions: 0
Ack responses: 0, Nak reponses: 0
invalid requests: 0, errors: 0
Average Ack response time: 0 msec

Details of counters displayed:
1. Requests – Counts the Requests received from CoA clients
2. transactions – Counts CoA completed transactions. A Completed transaction occurs once
the Switch send an ACK or NAK in response to a Request from a CoA client.
3. Retransmissions – Counts received retransmitted CoA Requests. A retransmitted CoA Requests
 is a Request in which the Request identifier is identical to the identifier of a previous
 Request.
4. active transactions – Transactions that are currently active. An active transaction is
a transaction in which a Request from a COA Client has been received but an ACK or NAK
response has not been sent yet. Once an ACK or NAK is sent this counter is decremented.
5. Ack responses - Counts the number of Ack responses sent by the switch.
6. Nak responses - Counts the number of Nak responses sent by the switch
7. invalid requests – Counts invalid requests received by the switch. An invalid request
is one of the following
    a) A Request in which the secret in the Request does not match the Secret configured
on the device,
    b) A Request with no session identifier
    c) A Request with an unsupported attribute
    d) A Request in which a supported attribute is empty
    e) A Request which is discarded because the event-timestamp is not current, or if
event-timestamp is mandatory and received request does not include this attribute
    f) A Request with a not current or missing Event-Timestamp attribute
    g) A request received with “disable port” or “bounce port” command that are dropped due
 to user configuration.
8. errors – Counts errors. an error can be an internal error in which a request cannot be
```

```
processed due to resource issue, or if a secret has not been configured for the CoA client
9. Average Ack response time – in milliseconds
```

clear aaa counters clients

Use the clear aaa counters clients Privilege EXEC mode command to clear AAA (CoA) clients' statistics

Syntax

clear aaa counters clients [ip-address]

Parameters

- *ip-address* (optional) — Clears the statistics for a specific CoA client host. The IP address can be an IPv4, IPv6 or IPv6z address.

Default Configuration

By default, the statistics of all CoA clients are clears.

Command Mode

Privileged EXEC mode

Examples

```
Switch010203# clear aaa counters clients
```

show aaa server radius dynamic-author

Use the show aaa server radius dynamic-author Privilege EXEC mode command to show CoA configuration.

Syntax

show aaa server radius dynamic-author *[ip-address]*

Parameters

ip-address—Specifies the CoA client host IP address to display. The IP address can be an IPv4, IPv6 or IPv6z address.

Command Mode

Privileged EXEC mode

Default Configuration

By default, the command displays the information for all configured CoA clients.

Examples

Example 1

```
Switch010203# show aaa server radius dynamic-author
CoA UDP port: 1700
Default Server-Key MD5: 9aa6e5f2256c17d2d430b100032b997c
Ignore Server-Key: disabled
Domain delimiter: @
Domain stripping: disabled
“disable port” command: process
“bounce port” command: process
Event-Timestamp attribute drop packet: disabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2
1111::1100	default

Example 2

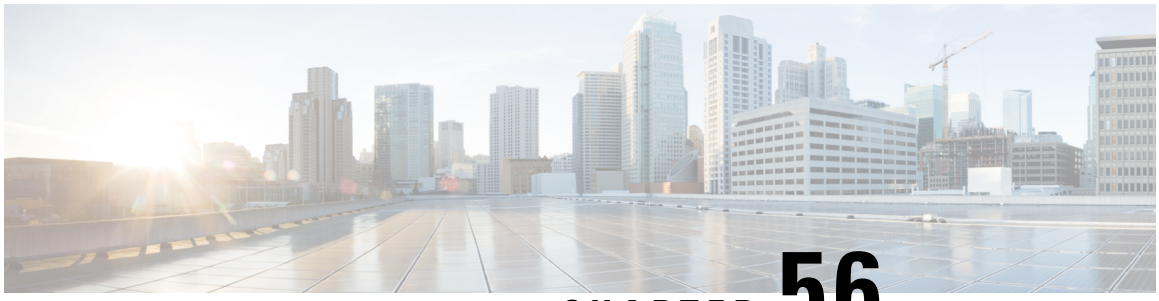
```
Switch010203# show aaa server radius dynamic-author
CoA UDP port: 1968
Default Server-Key MD5: Not configured
Ignore Server-Key: enabled Domain delimiter: $
Domain stripping: enabled (left to right) “disable port” command: ignore
“bounce port” command: process
Event-Timestamp attribute drop packet: enabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2
1111::1100	default

Example 3

```
Switch010203# show aaa server radius dynamic-author 1.1.1.1
CoA UDP port: 1977
Default Key MD5: Not configured
Ignore Server-Key: enabled Domain delimiter: $
Domain stripping: enabled (left to right)
“disable port” command: process
“bounce port” command: ignore
Event-Timestamp attribute drop packet: disabled
```

CoA Client Address	Server-Key's MD5
1.1.1.1	02cea75e335fcb814cd81932f1c15dc2



CHAPTER 56

Radius Server Commands

This chapter contains the following sections:

- allowed-time-range, on page 899
- clear radius server accounting, on page 900
- clear radius server rejected users, on page 901
- clear radius server statistics, on page 901
- clear radius server unknown nas, on page 902
- privilege-level, on page 902
- radius server accounting-port, on page 903
- radius server authentication-port, on page 903
- radius server enable, on page 904
- radius server group, on page 905
- radius server nas secret, on page 905
- radius server traps accounting, on page 907
- radius server traps authentication success, on page 907
- radius server user, on page 908
- show radius server accounting, on page 909
- show radius server configuration, on page 910
- show radius server group, on page 911
- show radius server rejected users, on page 911
- show radius server nas secret, on page 912
- show radius server statistics, on page 913
- show radius server unknown nas, on page 915
- show radius server user, on page 915
- vlan, on page 916

allowed-time-range

To define the time user can connect, use the **allowed-time-range** command in Radius Server Group Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

allowed-time-range *time-range-name*

no allowed-time-range

Parameters

- ***time-range-name***—Specifies the time range name configured by the time range command.

Command Mode

Radius Server Group Configuration mode

User Guidelines

Use the **allowed-time-range** command, to define the time users can connect.

Use the **no** form of the command, to return to the default.

Example

The following example assigns an periodical time interval:

```
switchxxxxxx(config)# time-range connection-time
switchxxxxxx(config-time-range)# periodic mon 12:00 to wed 12:00
switchxxxxxx(config-time-range)# exit
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# allowed-time-range connection-time
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

clear radius server accounting

To clear the Radius Accounting cache, use the **clear radius server accounting** command in Privileged EXEC mode.

Syntax

clear radius server accounting

Command Mode

Privileged EXEC mode

User Guidelines

Use the **clear radius server accounting** command, to clear the Radius Accounting cache.

Example

The following example clears the Radius Accounting cache:

```
switchxxxxxx(config)# clear radius server accounting
```

clear radius server rejected users

To clear the Radius Rejected Users cache, use the **clear radius server rejected users** command in Privileged EXEC mode.

Syntax

clear radius server rejected users

Command Mode

Privileged EXEC mode

User Guidelines

Use the **clear radius server rejected users** command, to clear the Radius Rejected Users cache.

Example

The following example clears the Radius Rejected Users cache:

```
switchxxxxxx(config)# clear radius server rejected users
```

clear radius server statistics

To clear the Radius server counters, use the **clear radius server statistics** command in Privileged EXEC mode.

Syntax

clear radius server statistics [*ip-address*]

Parameters

- *ip-address*—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **clear radius server statistics** command without parameter to clear the all counters.

Use the **clear radius server statistics** command with parameter to clear the counters of a given NAS.

Example

The following example clears the Radius server counters:

```
switchxxxxxx(config)# clear radius server statistics
```

clear radius server unknown nas

To clear the Radius Unknown NAS cache, use the **clear radius server unknown nas** command in Privileged EXEC mode.

Syntax

clear radius server unknown nas

Command Mode

Privileged EXEC mode

User Guidelines

Use the **clear radius server unknown nas** command, to clear the Radius Unknown NAS cache.

Example

The following example clears the Radius Unknown NAS cache:

```
switchxxxxxx(config)# clear radius server unknown nas
```

privilege-level

To define the user privilege level, use the **privilege-level** command in Radius Server Group Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

privilege-level *level*

no privilege-level

Parameters

- ***level***—Specifies the user privilege level. (Range: 1-15)

Default Configuration

1

Command Mode

Radius Server Group Configuration mode

User Guidelines

Use the **privilege-level** command, to define the privilege level of users of the given group.

Use the **no** form of the command, to return to the default.

A value of privilege level is passed to a Radius client in the Access-Accept message in the Vendor-Specific(26) attribute. The attribute is only passed to login users.

Example

The following example specified privilege level 15 for users of the developers group:

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# privilege-level 15
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```

radius server accounting-port

To define the accounting UDP port used for accounting requests, use the **radius server accounting-port** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

radius server accounting-port udp-port

no radius server accounting-port

Parameters

- *udp-port*—Specifies the UDP port number for accounting requests. (Range: 1–59999)

Default Configuration

1813

Command Mode

Global Configuration mode

User Guidelines

Use the **radius server accounting-port** command, to define an UDP port for accounting requests.

Use the **no radius server accounting-port** command, to restore the default UDP accounting port.

Example

The following example defines port 2083 as an accounting UDP port:

```
switchxxxxxx(config)# accounting-port 2083
```

radius server authentication-port

To define the authentication UDP port used for authentication requests, use the **radius server authentication-port** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

radius server authentication-port udp-port

no radius server authentication-port

Parameters

- *udp-port*—Specifies the UDP port number for authentication requests. (Range: 1–59999)

Default Configuration

1812

Command Mode

Global Configuration mode

User Guidelines

Use the **radius server authentication-port** command, to define an UDP port for authentication requests.

Use the **no radius server authentication-port** command, to restore the default UDP authentication port.

Example

The following example defines port 2083 as an authentication UDP port:

```
switchxxxxxx(config)# authentication-port 2083
```

radius server enable

To enable Embedded Radius server, use the **radius server enable** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

radius server enable

no radius server enable

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

Use the **radius server enable** command, to enable Embedded Radius server.

Use the **no radius server enable** command, to disable Embedded Radius server.

Example

The following example enables Embedded Radius server:

```
switchxxxxxx(config)# radius server enable
```

radius server group

To enter into Radius Server Group Configuration mode and create this group if it does not exist, use the **radius server group** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

radius server group group-name

no radius server group *[group-name*]

Parameters

- ***group-name***—Specifies a name of the group. (Length: 1–32 characters)

Default Configuration

The group does not exist.

Command Mode

Global Configuration mode

User Guidelines

Use the **radius server group** command, to enter into the Radius Server Group Configuration mode. If this group does not exist it is created automatically.

Use the **no radius server group** group-name command, to delete one group.

Use the **no radius server group** command, to delete all groups.

A group cannot be deleted, if there is a user referencing to this group.

The Radius server supports up to 50 groups.

Example

The following example creates group developers, if it does not exist, and enters into its context:

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)#
```

radius server nas secret

To create a secret key, use the **radius server nas secret key** command in Global Configuration mode. To delete the key, use the **no** form of this command.

Syntax

radius server nas secret key key {**default** | *ip-address*}

radius server nas secret ip-address

encrypted radius server nas secret key *encrypted-key* {**default** | *ip-address*}

no radius server nas secret *[***default** | *ip-address*]

Parameters

- ***key***—Specifies the authentication and encryption key for communications between the device and users of the given group. (Range: 0–128 characters)
- ***encrypted-key***—Same as the key-string parameter, but the key is in encrypted form.
- **default**—Specifies the default secret key that will be applied to communicate with NASs that do not have a private key.
- *ip-address*—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

Default Configuration

The secret key does not exist.

Command Mode

Global Configuration mode

User Guidelines

Use the **radius server nas secret key** key **default** command, to defines a key that will be applied to communicate with NASs that do not have a private key.

Use the **radius server nas secret key** key *ip-address* command, to defines a key that will be applied to communicate with the specified NAS.

Use the **radius server nas secret** ip-address command, to defines that the default secret key will be applied to communicate with the specified NAS.

If a NAS is not defined by this command all messages received from this NAS will be dropped.

The Radius server supports up to 50 NASs.

Use the **no radius server nas secret default** command, to delete the default key.

Use the **no radius server nas secret** ip-address command, to remove the given NAS and its secret key.

Use the **no radius server nas secret** command, to delete all NASs and all secret keys.

Example 1. The following example defines a default secret key:

```
switchxxxxxx(config)# radius server nas secret key qrBut56$#qw default
```

Example 2. The following example defines a default secret key:

```
switchxxxxxx(config)# radius server nas secret key qrBut56$#qw default
```

Example 3. The following example defines a NAS using the default secret key:

```
switchxxxxxx(config)# radius server nas secret 10.05.10.1
```

radius server traps accounting

To enable sending accounting traps, use the **radius server traps accounting** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

Syntax

radius server traps accounting

no radius server traps accounting

Default Configuration

Accounting traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending accounting traps:

```
switchxxxxxx(config)# radius server traps accounting
```

radius server traps authentication success

To enable sending traps when a user is successfully authorized, use the **radius server traps authentication success** command in Global Configuration mode. To disable the traps, use the **no** form of this command.

Syntax

radius server traps authentication success

no radius server traps authentication success

Default Configuration

Success traps are disabled.

Command Mode

Global Configuration mode

User Guidelines

A rate limit is applied to the traps: not more than one trap of this type can be sent in 10 seconds.

Example

The following example enables sending traps when a user is successfully authorized:

```
switchxxxxxx(config)# radius server traps authentication success
```

radius server user

To create a user, use the **radius server user** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

radius server user username user-name **group** group-name **password** *unencrypted-password*

encrypted radius server user username user-name **group** *group-name* **password***encrypted-password*

no radius server user *[***username** user-name | **group** group-name]

Parameters

- ***user-name***—Specifies the user name. (Length: 1–32 characters)
- ***group-name***—Specifies the user group name. (Length: 1–32 characters)
- ***unencrypted-password***—Specifies the user password. (Length: 1–64 characters)
- ***encrypted-password***—Same as the *unencrypted-password* parameter, but the password is in the encrypted form.

Default Configuration

The user does not exist.

The Radius server supports up to 1024 users.

Command Mode

Global Configuration mode

User Guidelines

Use the **radius server user** command, to create a new user.

Use the **no radius server user username** user-name command to delete one user.

Use the **no radius server user group** group-name command to delete users of the given group.

Use the **no radius server user** command to delete all users.

Example

Example 1. The following example creates a new user with name bob of group developer with password Aerv#136dSsT:

```
switchxxxxxx(config)# radius server user username bob group developers password Aerv#136dSsT
```

Example 2. The following example creates a new user with name bill of group finance and the password is provided in the encrypted format:

```
switchxxxxxx(config)# encrypted radius server user username bill group
finance password bCWG7DnKMNUaik4S0TkLDkJVYIsQcwQkRFVYj7VNvAI=
```

show radius server accounting

To display user accounting information, use the **show radius server accounting** command in Privileged EXEC mode.

Syntax

show radius server accounting *[***username** *user-name*]

Parameters

- ***user-name***—Specifies the user name. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

User Guidelines

The Radius server saves the last 1024 accounting logs in a cycle file on FLASH.

Use the **show radius server accounting username** *user-name* command, to display accounting information of one user.

Use the **show radius server accounting** command, to display accounting information of all users.

Example 1. The following example displays accounting information of all users:

```
switchxxxxxx# show radius server accounting
29-Jun-14, 16:00, Stop
  User: Bob
  Accounting Session Time: 6 hours,15 minutes
  Authenticated by: local
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
  Termination Reason: User Request
29-Jun-14, 12:04, Start
  User: Alisa
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 00:12:cf:00:1c:25
  NAS Port: 10
29-Jun-14, 12:04, Stop
  User: Alisa
```

```
  Accounting Session Time: 2 days,2 hours,10 minutes
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 00:12:cf:00:1c:25
  Termination Reason: User Request
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-2014, 9:05, Start
  User: Bob
  Authenticated by: local
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
*20-Feb-2008, 9:00, Reboot
```

Example 2. The following example displays accounting information of one user Bob:

```
switchxxxxxx# show radius server accounting username Bob:
29-Jun-14, 16:00, Stop
  User: Bob
  Accounting Session Time: 6 hours,15 minutes
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
  Termination Reason: User Request
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-2014, 9:05, Start
  User: Bob
  Authenticated by: Radius
  NAS Address: 10.23.1.3
  User Address: 160.134.7.8
*20-Feb-2008, 9:00, Reboot
```

show radius server configuration

To display Radius Server global configuration, use the **show radius server configuration** command in Privileged EXEC mode.

Syntax

show radius server configuration

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show radius server configuration** command, to display Radius server global configuration.

Example

The following example displays radius server global configuration:

```
switchxxxxxx# show radius server configuration
Radius Server Status: Enabled
Authentication UDP port: 1812 (default)
Accounting UDP port: 1813 (default)
Authentication failure traps are enabled
```

```
Authentication success traps are enabled
Accounting traps are enabled
```

show radius server group

To display a Radius Server group configuration, use the **show radius server group** command in Privileged EXEC mode.

Syntax

show radius server group *[group-name]*

Parameters

- ***group-name***—Specifies a name of the group. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show radius server group** *group-name* command, to display one group.

Use the **show radius server group** command, to display all groups.

Example

The following example displays radius server groups.

```
switchxxxxxx# show radius server group
Group gr1
  VLAN: 124
  Privilege Level: 15
  Time Range: ConnectionTime
  Group Users: develop, designers
Group gr2
  Privilege Level: 1 (default)
  Group Users: bob
```

show radius server rejected users

To display rejected users, use the **show radius server rejected users** command in Privileged EXEC mode.

Syntax

show radius server rejected users *[***username** *user-name]*

Parameters

- ***user-name***—Specifies the user name. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

User Guidelines

The Radius server saves the last 1024 rejected authentication requests in a cycle file on FLASH.

The Radius server saves the last 1024 accounting logs in a cycle file on FLASH.

Use the **show radius server rejected users** *user-name* command, to display one rejected user.

Use the **show radius server rejected users** command, to display all rejected users.

Example 1. The following example displays all rejected users:

```
switchxxxxxx# show radius server rejected users
30-Jun-14 16:44
  User Name: Jack
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Unknown user
30-Jun-14 16:04
  User Name: Bob
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Illegal password
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-08 16:24
  User Name: Robert
  User Type: 802.1x
  NAS Address: 10.1.1.1
  NAS Port: 2
  User Address: 00:67:67:96:ac:21
  Reason: Not Supported EAP method
20-Feb-08 14:14
  User Name: Alisa
  User Type: 802.1x
  NAS Address: 10.1.1.1
  NAS Port: 2
  User Address: 00:67:67:96:ac:21
  Reason: Not allowed at this time
*20-Feb-2008, 9:00, Reboot
```

Example 2. The following example displays one rejected user Bob:

```
switchxxxxxx# show radius server rejected users 30-Jun-14 16:04
  User Name: Bob
  User Type: Login
  NAS Address: 10.1.1.1
  User Address: 10.23.4.3
  Reason: Illegal password
*20-Feb-2008, 9:20, Date and Time were updated to 29-Jun-14, 11:00
*20-Feb-2008, 9:00, Reboot
```

show radius server nas secret

To display secret keys, use the **show radius server nas secret** command in Privileged EXEC mode.

Syntax

show radius server nas secret *[***default** | ***ip-address***]

Parameters

- **default**—Specifies the default secret key hat will be applied to communicate with NASs that do not have a private key.
- ***ip-address***—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show radius server nas secret default** command, to display the default secret key.

Use the **show radius server nas secret** ip-address command, to display the given NAS secret key.

Use the **show radius server nas secret** command, to display all secret keys.

Example 1. The following example displays all secret keys:

```
switchxxxxxx# show radius server nas secret
Default Secret Key's MD5:1238af77aaca17568f1298cced1255cc
    NAS Address                Secret Key's MD5
-------------------------  --------------------------------
10.1.35.3                  1238af77aaca17568f1298cced165fec
10.2.37.6                  default
3000:1231:1230:9cab:1384   1238af77aaca17568f12988601fcabed
3001:ab11::9cda:0981       1238af77aaca17568f1298bc5476ddad
```

Example 2. The following example displays the default secret key:

```
switchxxxxxx# show radius server nas secret default
Default Secret Key's MD5:1238af77aaca17568f1298cced1255cc
```

Example 3. The following example displays the secret key of one given NAS:

```
switchxxxxxx# show radius server nas secret 10.1.35.3
           NAS ID                Secret Key's MD5
-------------------------  --------------------------------
10.1.35.3                  1238af77aaca17568f1298cced165fec
```

show radius server statistics

To display the Radius server counters, use the **show radius server statistics** command in User EXEC mode.

Syntax

show radius server statistics [***ip-address***]

Parameters

- ***ip-address***—Specifies the RADIUS client host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.

Command Mode

User EXEC mode

User Guidelines

Use the **show radius server statistics** command to display the Radius server counters defined in RFC4669 and RFC4671.

Use the **show radius server statistics** command without parameter to display the global counters.

Use the **show radius server statistics** command with parameter to display the counters of the given NAS.

Example 1. The following example displays the Radius server global counters:

```
switchxxxxxx# show radius server statistics
Number of incoming packets on the authentication port: 120
Number of incoming Access-Requests from unknown addresses: 0
Number of duplicate incoming Access-Requests: 3
Number of sent Access-Accepts: 100
Number of sent Access-Rejects: 17
Number of sent Access-Challenges: 0
Number of incoming malformed Access-Requests: 0
Number of incoming Authentication-Requests with Bad Authenticator: 0
Number of incoming Authentication packets with other mistakes: 0
Number of incoming Authentication packets of unknown type: 0
Number of incoming packets on the accounting port: 80
Number of incoming Accounting-Requests from unknown addresses: 12
Number of incoming Accounting-Requests from unknown addresses: 0
Number of incoming duplicate Accounting-Requests: 0
Number of sent Accounting-Responses: 0
Number of incoming malformed Accounting-Requests: 0
Number of incoming Accounting-Requests with Bad Authenticator: 0
Number of incoming Accounting packets with other mistakes: 0
Number of incoming not recorded Accounting-Requests: 0
Number of incoming Accounting packets of unknown type: 0
```

Example 2. The following example displays the Radius server counters of the given SNA: secret keys:

```
switchxxxxxx# show radius server statistics 1.1.1.1
NAS: 1.1.1.1
Number of incoming packets on the authentication port: 120
Number of duplicate incoming Access-Requests: 3
Number of sent Access-Accepts: 100
Number of sent Access-Rejects: 17
Number of sent Access-Challenges: 0
Number of incoming malformed Access-Requests: 0
Number of incoming Authentication-Requests with Bad Authenticator: 0
Number of incoming Authentication packets with other mistakes: 0
Number of incoming Authentication packets of unknown type: 0
Number of incoming packets on the accounting port: 80
Number of incoming Accounting-Requests from unknown addresses: 0
Number of incoming duplicate Accounting-Requests: 0
Number of sent Accounting-Responses: 0
Number of incoming malformed Accounting-Requests: 0
Number of incoming Accounting-Requests with Bad Authenticator: 0
```

```
Number of incoming Accounting packets with other mistakes: 0
Number of incoming not recorded Accounting-Requests: 0
Number of incoming Accounting packets of unknown type: 0
```

show radius server unknown nas

To display unknown NASes, use the **show radius server unknown nas** command in Privileged EXEC mode.

Syntax

show radius server unknown nas

Command Mode

Privileged EXEC mode

User Guidelines

The Radius server saves the last 100 unknown NASes in a cycle cache.

Example

The following example displays Radius requests received from unknown NASes:

```
switchxxxxxx# show radius server unknown nas
30-Jun-14 16:44 NAS Address: 10.1.1.1
30-Jun-14 16:04 NAS Address: 10.1.1.1
*20-Feb-08, 9:20, Date and Time were updated to 29-Jun-14, 11:00
20-Feb-08 16:24 NAS Address: 10.1.1.1
20-Feb-08 14:14 NAS Address: 10.1.1.1
*20-Feb-08, 9:00, Reboot
```

show radius server user

To display a Radius Server user configuration, use the **show radius server user** command in Privileged EXEC mode.

Syntax

show radius server user *[***username** *user-name*] | [**group** *group-name*]

Parameters

- ***user-name***—Specifies the user name. (Length: 1–32 characters)
- ***group-name***—Specifies a name of the group. (Length: 1–32 characters)

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show radius server user username** *user-name* command, to display one user.

Use the **show radius server user group** *group-name* command, to display all users of the given group.

Use the **show radius server user** command, to display all users.

Examples

The following example displays one user bob:

```
switchxxxxxx# show radius server user username bob
User bob
  Group: developers
  Password's MD5: 1238af77aaca17568f1298cced1255cc
```

vlan

To define Radius Assigned VLAN, use the **vlan** command in Radius Server Group Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

vlan {**id** *vlan-id* | **name** *vlan-name*}

no vlan

Parameters

- ***vlan-id***—Specifies a VLAN ID. (Range: 1-4094)
- ***vlan-name***—Specifies a name of the VLAN. (Length: 1–32characters)

Default Configuration

No Radius Assigned VLAN.

Command Mode

Radius Server Group Configuration mode

User Guidelines

Use the **vlan** command, to assign the VLAN to a radius client. This Radius Assigned VLAN is passed to a Radius client in the Access-Accept message in the following attributes:

- Tunnel-Type(64)
- Tunnel-Medium-Type(65)
- Tunnel-Private-Group-ID(81)

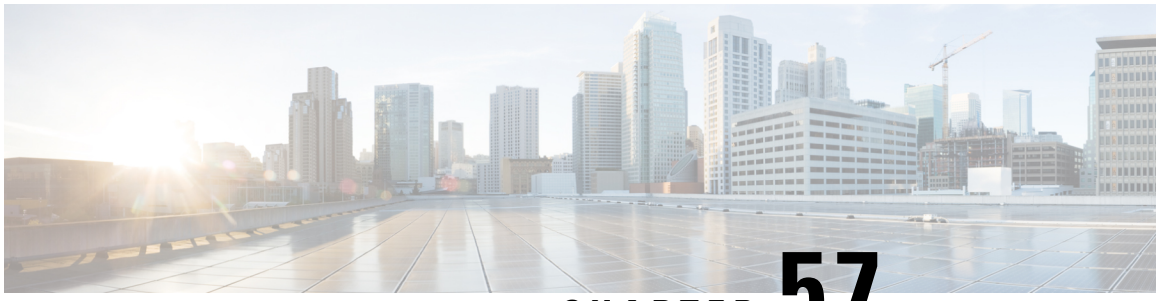
If a VLAN is not assigned these attributes are not included in the Access-Accept message.

Use the **no** form of the command, to delete VLAN assignment.

Example

The following example assigns VLAN 100 to users of the developers group and VLAN with name management of users of the managers group:

```
switchxxxxxx(config)# radius server group developers
switchxxxxxx(config-radser-group)# vlan id 100
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)# radius server group managers
switchxxxxxx(config-radser-group)# vlan name management
switchxxxxxx(config-radser-group)# exit
switchxxxxxx(config)#
```



CHAPTER 57

Rate Limit and Storm Commands

This chapter contains the following sections:

- clear storm-control counters, on page 919
- rate-limit (Ethernet), on page 920
- rate-limit vlan, on page 921
- storm-control, on page 922
- show rate-limit interface, on page 923
- show rate-limit vlan, on page 923
- show storm-control interface, on page 924

clear storm-control counters

To clear storm control counters, use the **clear storm-control counters** command in Privileged EXEC mode.

Syntax

clear storm-control counters [**broadcast** | **multicast** | **unicast**] [interface *interface-id*]

Parameters

- **broadcast**—(Optional) Clear Broadcast storm control counters.
- **multicast**—(Optional) Clear Multicast storm control counters.
- **unicast**—(Optional) Clear Unicast Unknown storm control counters.
- **interface** *interface-id*—(Optional) Clear storm control counters for the specified Ethernet port.

Command Mode

Privileged EXEC mode

User Guidelines

The switch clears the port counter of a given traffic type when storm control for this traffic type on this port is enabled.

Use this command to clear the storm control counters when storm control is running.

Use the **clear storm-control counters** command to clear all the storm control counters of all Ethernet ports.

Use the **clear storm-control counters interface** *interface-id* command to clear all the storm control counters of a given port.

Use the **clear storm-control counters broadcast** | **multicast** | **unicast** command to clear all storm control counters of a given traffic type of all Ethernet ports.

Use the **clear storm-control counters broadcast** | **multicast** | **unicast interface** *interface-id* command to clear one storm control counter of a given traffic type and of a given port.

Example 1. The following example clears all storm control counters of all ports:

```
switchxxxxxx# clear storm-control counters
```

Example 2. The following example clears all storm control counters of port gi1/0/1:

```
switchxxxxxx# clear storm-control counters interface gi1/0/1
```

Example 3. The following example clears broadcast storm control counter of all ports:

```
switchxxxxxx# clear storm-control counters broascat
```

Example 4. The following example clears multicast storm control counter of port gi1/0/1:

```
switchxxxxxx# clear storm-control counters multicast interface gi1/0/1
```

rate-limit (Ethernet)

To limit the incoming traffic rate on a port, use the **rate-limit** command in Interface (Ethernet) Configuration mode. To disable the rate limit, use the **no** form of this command.

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–maximal port speed.
- **burst** *committed-burst-bytes*—(Optional) The burst size in bytes. (Range: 3000–19173960). If unspecified, defaults to 128K.

Default Configuration

Rate limiting is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

The Rate Limit does not calculate traffic controlled by Storm control. The real allowed rate will be sum of the rate specified by the command and the rates specified by the Storm control commands for particular traffic types.

Example

The following example limits the incoming traffic rate on gi1/0/1 to 150,000 kbps.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# rate-limit 150000
```

rate-limit vlan

To limit the incoming traffic rate for a VLAN in, use the **rate-limit vlan** command in Global Configuration mode. To disable the rate limit, use the **no** form of this command.

Syntax

rate-limit vlan *vlan-id committed-rate committed-burst-bytes*

no rate-limit vlan *vlan-id*

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.

Command Mode

Global Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

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.

VLAN Rate limiting is calculated separately for each unit in a stack.

It does not work in conjunction with IP Source Guard.

Example

The following example limits the rate on VLAN 11 to 150000 kbps and the committed burst size to 9600 bytes.

```
switchxxxxxx(config)# rate-limit vlan 11 150000 9600
```

storm-control

To enable broadcast, multicast, or unicast storm control on a port, use the **storm-control** command in Interface (Ethernet) Configuration mode. To return to default, use the **no** form of this command.

Syntax

storm-control broadcast {**level** *level* | **kbps** *kbps***} [trap**] [**shutdown**]

no storm-control broadcast

storm-control multicast [**registered** | **unregistered**] {**level** *level* | **kbps** *kbps***} [trap**] [**shutdown**]

no storm-control multicast

storm-control unicast {**level** *level* | **kbps** *kbps***} [trap**] [**shutdown**]

no storm-control unicast

no storm-control

Parameters

- **broadcast**—Enables broadcast storm control on the port.
- **multicast** [**registered** | **unregistered**]—Enables either all multicast, only registered multicast, or only unregistered multicast storm control on the port.
- **unicast**—Enables unicast unknown storm control on the port.
- **level** *level*—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1-100)
- **kbps** *kbps*—Maximum of kilobits per second of Broadcast traffic on a port. (Range 1 –10000000)
- **trap**—(Optional) Sends a trap when a storm occurs on a port. If the keyword is not specified the trap is not sent.
- **shutdown**—(Optional) Shut down a port when a storm occurs on the port. If the keyword is not specified extra traffic is discarded.

Default Configuration

Storm control is disabled.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

The calculated rate includes the 20 bytes of Ethernet framing overhead (preamble+SFD+IPG).

The rate limit on a port does not calculate traffic controlled by storm control on this port.

Use the **no storm-control** command to disable storm control of all traffic type on the port.

Example

The following example enables broadcast, multicast, and unicast unknown storm control on port gi1/0/1 and multicast unregistered and unicast unknown on port gi1/0/2:

Enable group 1 for registered and unregistered multicast traffic on interface gi1/0/1. Extra traffic is discarded.

switchxxxxxx(config)# **interface gi1/0/1** switchxxxxxx(config-if)# **storm-control broadcast kbps 10000 shutdown** switchxxxxxx(config-if)# **storm-control multicast level 20 trap** switchxxxxxx(config-if)# **storm-control unicast level 5 trap shutdown** switchxxxxxx(config-if)# **exit** switchxxxxxx(config)# **interface gi1/0/2** switchxxxxxx(config-if)# **storm-control multicast unregistered level 5 trap shutdown** switchxxxxxx(config-if)# **storm-control unicast level 5 trap** switchxxxxxx(config-if)# **exit**

show rate-limit interface

To display rate limit configuration on an interface, use the **show rate-limit interface** command in Privileged EXEC mode.

Syntax

show rate-limit interface [*interface-id***]**

Parameters

- ***interface-id***—(Optional) Specifies an Ethernet port. If the argument is not configured rate limit configuration of all Ethernet ports is displayed.

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the **show rate-limit interface**:

```
switchxxxxxx> show rate-limit interface
```

Interface	Rate Limit (kbps)	Burst (Bytes)
----------	----------	----------
gi1/0/1gi1/0/2	80000	512
	100000	1024

show rate-limit vlan

To display rate limit configuration on a VLAN, use the **show rate-limit vlan** command in Privileged EXEC mode.

Syntax

show rate-limit vlan [*vlan-id***]**

Parameters

- ***vlan-id***—(Optional) Specifies a VLAN ID If the argument is not configured rate limit configuration of all VLANs is displayed.

Default Configuration

N/A

Command Mode

Privileged EXEC mode

Examples

The following is an example of the output from the **show rate-limit vlan**:

```
switchxxxxxx> show rate-limit vlan 1075
```

VLAN	Rate Limit (kbps)	Burst (Bytes)
--------	----------	----------
1075	100000	1024

show storm-control interface

To display storm control information of an interface, use the **show storm-control interface** command in Privileged EXEC mode.

Syntax

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

Parameters

- ***interface-id***—(Optional) Specifies an Ethernet port. If the argument is not configured storm control information of all Ethernet ports is displayed.

Command Mode

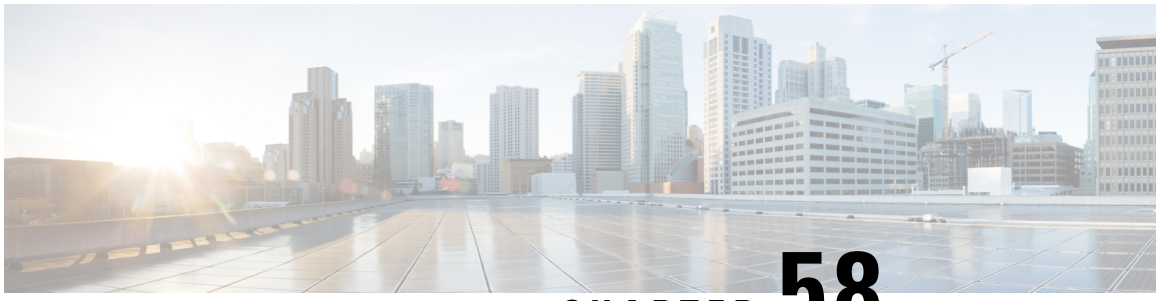
Privileged EXEC mode

Examples

The following is an example of the output from the **show storm-control interface**:

```
switchxxxxxx> show storm-control interface
gi1/0/1
 Broadacst
```

```
 Rate: 5%
 Action: Shutdown
 Passed Counter (Bytes): 124997
 Dropped Counter (Bytes): 10
 Last drop time: 27-Jan-2014, 09:00:01
 Multicast
 Rate: 1000 kbps
 Action: Drop, Trap
 Passed Counter (Bytes):112876
 Dropped Counter (Bytes):1272
 Last drop time: 20-Jan-2014, 11:00:01
 Unicast
 Rate: 10%
 Action: drop
 Passed Counter (Bytes): 27653
 Dropped Counter (Bytes):1
 Last drop time: 27-Feb-2014, 09:00:01
gi1/0/2
 Broadacst
 Rate: 5%
 Action: Shutdown
 Passed Counter (Bytes): 124997
 Dropped Counter (Bytes): 0
 Last drop time:
 Multicast Unregistred
 Rate: 5%
 Action: Shutdown
 Traffic Type:Broadcast
 Passed Counter (Bytes): 124997
 Dropped Counter (Bytes): 3
 Last drop time: 26-Jan-2014, 10:00:01
```



CHAPTER 58

RIP Commands

This chapter contains the following sections:

- clear rip statistics, on page 927
- default-information originate, on page 928
- default-metric, on page 928
- ip rip authentication key-chain, on page 929
- ip rip authentication mode, on page 930
- ip rip authentication-key, on page 931
- ip rip default-information originate, on page 932
- ip rip distribute-list in, on page 932
- ip rip distribute-list out, on page 933
- ip rip offset, on page 934
- ip rip passive-interface, on page 934
- ip rip distribute-list in, on page 935
- ip rip distribute-list out, on page 936
- ip rip offset, on page 937
- ip rip passive-interface, on page 937
- ip rip shutdown, on page 938
- network, on page 938
- passive-interface (RIP), on page 939
- redistribute (RIP), on page 940
- router rip, on page 942
- show ip rip database, on page 942
- show ip rip peers, on page 944
- show ip rip statistics, on page 945
- shutdown , on page 945

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

Command Mode

Privileged EXEC mode

Example

The following example shows how to clear all counters:

```
switchxxxxxx# clear rip statistics
```

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

no default-information originate

Default Configuration

Default route is not generated by RIP.

Command Mode

Router RIP Configuration mode

User Guidelines

Use the command to enable generation of a default route.

Example 1 - The following example shows how to originate a default route:

switchxxxxxx(config)# router rip switchxxxxxx(config-rip)# default-information originate
switchxxxxxx(config-rip)# exit

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. Range 1-15.

Default Configuration

metric-value—1.

Command Mode

Router RIP Configuration mode

Example

The following example shows how to set the default metric to 2:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# default-metric 2
switchxxxxxx(config-rip)# exit
```

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 Configuration 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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip authentication key-chain alpha
switchxxxxxx(config-route-map)# exit
```

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 Configuration 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:

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip authentication mode md5
switchxxxxxx(config-route-map)# exit
```

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 the 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 16 characters in length.

Default Configuration

No password is specified.

Command Mode

IP Configuration 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 IP interface. Each **ip rip authentication-key** command overrides the previous definition.

Example

The following example shows how to define a password:

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip authentication mode text
switchxxxxxx(config-route-map)# ip rip authentication-key alph$$12
switchxxxxxx(config-route-map)# exit
```

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 {disable | *metric*}

no ip rip default-information originate

Parameters ranges

- **disable**—Do not send the default route.
- ***metric***—Default route metric value. Range: 1-15.

Default Configuration

The RIP behavior is specified by the **default-information originate** command.

Command Mode

IP Configuration 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:

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip default-information originate 3
switchxxxxxx(config-route-map)# exit
```

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* **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.

Default Configuration

No filtering

Command Mode

IP Configuration 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. See the **ip access-list (IP standard)** and **ip prefix-list** commands for details.

Example

The following example shows how to define input filtering:

```
witchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 in
switchxxxxxx(config-route-map)# exit
```

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 rip distribute-list access *access-list-name* **out**

no ip rip distribute-list out

Parameters

- ***access-list-name***—Standard IP access list name, up to 32 characters. The list defines which routes in outgoing RIP update messages are to be sent and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP Configuration 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. See the **ip access-list (IP standard)** and **ip prefix-list** commands.

Example

The following example shows how to define outgoing filtering:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 out
switchxxxxxx(config-route-map)# exit
```

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. Range: 1-15.

Default Configuration

offset—1.

Command Mode

IP Configuration mode

User Guidelines

Example

The following example shows how to set offset to 2:

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# exit
```

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

Default Configuration

RIP messages are sent.

Command Mode

IP Configuration mode

User Guidelines

Use the **ip rip passive-interface** command to stop sending RIP messages on the giving IP interface. To stop RIP messages being sent 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 the sending of RIP messages:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

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* **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.

Default Configuration

No filtering

Command Mode

IP Configuration 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. See the **ip access-list (IP standard)** and **ip prefix-list** commands for details.

Example

The following example shows how to define input filtering:

```
witchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 in
switchxxxxxx(config-route-map)# exit
```

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 rip distribute-list access *access-list-name* **out**

no ip rip distribute-list out

Parameters

- ***access-list-name***—Standard IP access list name, up to 32 characters. The list defines which routes in outgoing RIP update messages are to be sent and which are to be suppressed.

Default Configuration

No filtering

Command Mode

IP Configuration 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. See the **ip access-list (IP standard)** and **ip prefix-list** commands.

Example

The following example shows how to define outgoing filtering:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip distribute-list access 5 out
switchxxxxxx(config-route-map)# exit
```

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. Range: 1-15.

Default Configuration

offset—1.

Command Mode

IP Configuration mode

User Guidelines

Example

The following example shows how to set offset to 2:

switchxxxxxx(config)# **interface ip** 1.1.1.1

```
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# exit
```

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

Default Configuration

RIP messages are sent.

Command Mode

IP Configuration mode

User Guidelines

Use the **ip rip passive-interface** command to stop sending RIP messages on the giving IP interface. To stop RIP messages being sent 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 the sending of RIP messages:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

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

Default Configuration

Enabled

Command Mode

IP Configuration 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:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip shutdown
switchxxxxxx(config-route-map)# exit
```

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.

Command Mode

Router RIP Configuration mode

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 1.The following example shows how to enable RIP on IP interface 1.1.1.1 with the default interface configuration:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 1.1.1.1
switchxxxxxx(config-rip)# exit
```

Example 2. The following example enables RIP on 1.1.1.1 in the shutdown state, configures metric and starts RIP:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 1.1.1.1 shutdown
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# ip rip offset 2
switchxxxxxx(config-route-map)# no ip rip shutdown
switchxxxxxx(config-route-map)# exit
```

passive-interface (RIP)

To disable sending routing updates on all RIP IP interfaces, use the **passive-interface** command in Router RIP Configuration mode. To re-enable the sending of RIP routing updates, use the **no** form of this command.

Syntax

passive-interface

no passive-interface

Default Configuration

Routing updates are sent on all IP RIP interfaces.

Command Mode

Router RIP Configuration mode

User Guidelines

After using 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 excludes the IP interface 1.1.1.1:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# passive-interface
switchxxxxxx(config-rip)# network 1.1.1.1
switchxxxxxx(config-rip)# network 2.2.2.2
switchxxxxxx(config-rip)# network 3.3.3.3
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-route-map)# no ip rip passive-interface
switchxxxxxx(config-route-map)# exit
```

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* [**metric** {*metric-value* | **transparent**}]

no redistribute *protocol*

Parameters

- ***protocol***—Source protocol from which routes are being redistributed. It can be one of the following keywords: **connected** or **static**.
- **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.

Default Configuration

Route redistribution is disabled

Command Mode

Router RIP Configuration mode

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.

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, 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.

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 1.The following example enables redistribution of static routes by RIP with transparent metric:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

Example 2. The following example enables redistribution of static routes by RIP with transparent metric and then changes the metric to default:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# no redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

Example 3. The following example enables redistribution of static routes by RIP with default metric and then changes the metric to transparent:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# exit
```

Example 4. The following example enables redistribution of static routes by RIP with transparent metric. The second redistribute command does not affect:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# redistribute static metric transparent
switchxxxxxx(config-rip)# redistribute static
switchxxxxxx(config-rip)# exit
```

Example 5. The following example disables redistribution of static routes by RIP:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# no redistribute static
switchxxxxxx(config-rip)# exit
```

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

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 this 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 can 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
```

show ip rip database

The **show ip rip database** Privileged EXEC mode command displays information about the RIP Database.

Syntax

show ip rip database [all | brief | *ip-address*]

Parameters

- **all**—Provides the full RIP database information about all RIP interfaces. The option is assumed if the parameter is omitted.
- **brief**—Provides a summary view of the RIP database information.
- ***ip-address***—Provides the full RIP database information about the given IP Address.

Command Mode

Privileged EXEC mode

Example 1—The following example shows the full RIP database information about all RIP interfaces is displayed:

```
switchxxxxxx# 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
Static:

Metric is transparent
IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
IP Interface: 2.2.2.2
Administrative State is enabled
IP Interface Offset is 2
No Default Originate Metric
Authentication Type is MD5
Key Chain Name is chain1
IN Filtering Type is Access List
Access List Name is 10
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:

```
switchxxxxxx# 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
Static
Metric is transparent

IP Interface: 1.1.1.1
Administrative State is enabled
IP Interface Offset is 10
Default Originate Metric is 12
Authentication Type is text
Password is afGRwitew%3
IN Filtering Type is Access List
Access List Name is 10
OUT Filtering Type is Access List
Access List Name is List12
```

Example 3—The following example shows the brief RIP database information about all RIP interfaces is displayed:

```
switchxxxxxx# show ip rip database brief
RIP is enabled
RIP Administrative state is UP
Default Originate Metric: route-map is condition
Default metric value is 1
Redistributing is enabled from
Connected
Metric is default-metric
Static
Metric is transparent


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    Access   Access
3.3.3.3         enabled     1      Yes
4.4.4.4         shutdown    1      No
```

Example 4—The following example shows the output when RIP is disabled:

```
switchxxxxxx# show ip rip database
RIP is disabled
```

show ip rip peers

The **show ip rip peers** Privileged EXEC mode command displays information about RIP Peers.

Syntax

show ip rip peers

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip rip peers
RIP is enabled
Static redistributing is enabled with Default metric
Default redistributing metric is 1
Address       Last          Received       Received
              Update        Bad Packets    Bad Route
------------  ---------     ----------     ---------
1.1.12        00:10:17          -                1
2.2.2.3       00:10:01          -             -
```

show ip rip statistics

The **show ip rip statistics** Privileged EXEC mode command displays RIP statistics.

Syntax

show ip rip statistics

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# show ip rip statistics
RIP is enabled
Static redistributing is enabled with transparent metric
Default redistributing metric is 1
Interface     Received       Received           Sent
              Bad            Bad                Triggered
              Pakets         Routes             Packets
------------  -------------  -------------      -----------
1.1.1.1            -                   1              8
2.2.2.2            -                   -              7
```

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

Default Configuration

Enabled

Command Mode

Router RIP Configuration mode

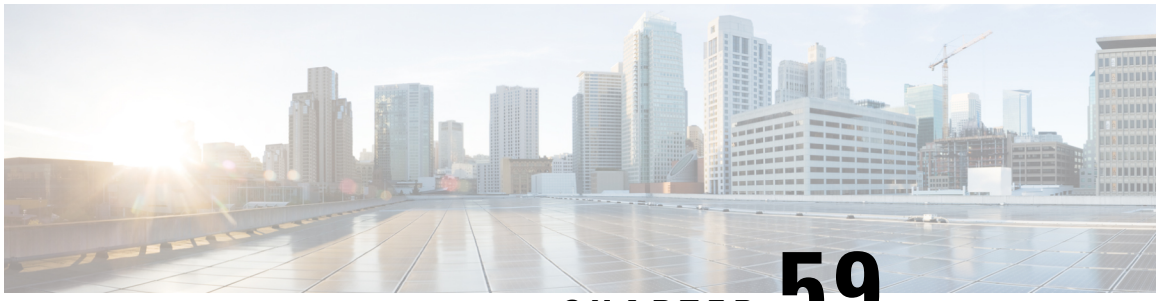
User Guidelines

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
```



CHAPTER 59

RMON commands

This chapter contains the following sections:

- rmon alarm, on page 947
- show rmon alarm-table, on page 948
- show rmon alarm, on page 949
- rmon event, on page 951
- show rmon events, on page 951
- show rmon log, on page 952
- rmon table-size, on page 953
- show rmon statistics, on page 954
- rmon collection stats , on page 956
- show rmon collection stats, on page 956
- show rmon history, on page 957

rmon alarm

To configure alarm conditions, use the **rmon alarm** Global Configuration modecommand. To remove an alarm, use the **no** form of this command.

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: 1–2147483647)
- **rising-threshold**—Specifies the rising threshold value. (Range: 0–2147483647)
- **falling-threshold**—Specifies the falling threshold value. (Range: 0–2147483647)

- **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**}—(Optional) 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**}—(Optional) 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*—(Optional) 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
```

show rmon alarm-table

To display a summary of the alarms table, use the **show rmon alarm-table** Privileged EXEC mode command.

Syntax

show rmon alarm-table

Parameters

This command has no arguments or keywords.

Command Mode

Privileged 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.

show rmon alarm

To display alarm configuration, use the **show rmon alarm** Privileged EXEC mode command.

Syntax

show rmon alarm *number*

Parameters

alarm *number*—Specifies the alarm index. (Range: 1–65535)

Command Mode

Privileged 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.

rmon event

To configure an event, use the **rmon event** Global Configuration modecommand. To remove an event, use the **no** form of this command.

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**—(Optional) Specifies the SNMP community (password) used when an SNMP trap is sent. (Octet string; length: 0–127 characters). Note this must be a community used in the definition of an SNMP host using the “snmp-server host” command.
- **description text**—(Optional) Specifies a comment describing this event. (Length: 0–127 characters)
- **owner name**—(Optional) 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
```

show rmon events

To display the RMON event table, use the **show rmon events** Privileged EXEC mode command.

Syntax

show rmon events

Parameters

This command has no arguments or keywords.

Command Mode

Privileged 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 ---------  ------  ------------------
2       High Broadcast Log      router      CLI       Jan 18 2006 23:58:17
                       Trap                 Manager   Jan 18 2006 23:59:48
```

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.

show rmon log

To display the RMON log table, use the **show rmon log** Privileged EXEC mode command.

Syntax

show rmon log [*event*]

Parameters

event—(Optional) Specifies the event index. (Range: 0–65535)

Command Mode

Privileged 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
```

rmon table-size

To configure the maximum size of RMON tables, use the **rmon table-size** Global Configuration modecommand. To return to the default size, use the no form of this command.

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: 20–32767)
- **log** *entries*—Specifies the maximum number of log table entries. (Range: 20–32767)

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
```

show rmon statistics

To display RMON Ethernet statistics, use the **show rmon statistics** Privileged EXEC mode command.

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

Privileged EXEC mode

Example

The following example displays RMON Ethernet statistics for port gi1/0/1.

```
switchxxxxxx#  show rmon statistics gi1/0/1
Port gi1/0/1
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).
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.

Field	Description
Multicast	Total number of good packets received and directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Align Errors	Total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	Best estimate of the total number of collisions on this Ethernet segment.
Undersize Pkts	Total number of packets received, less than 64 octets long (excluding framing bits, but including FCS octets) and otherwise well formed.
Oversize Pkts	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets) and otherwise well formed.
Fragments	Total number of packets received, less than 64 octets in length (excluding framing bits but including FCS octets) and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	Total number of packets received, longer than 1518 octets (excluding framing bits, but including FCS octets), and either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
64 Octets	Total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).
65 to 127 Octets	Total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128 to 255 Octets	Total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256 to 511 Octets	Total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512 to 1023 Octets	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024 to max	Total number of packets (including bad packets) received that were between 1024 octets and the maximum frame size in length inclusive (excluding framing bits but including FCS octets).

rmon collection stats

To enable RMON MIB collecting history statistics (in groups) on an interface, use the **rmon collection stats** Interface Configuration mode command. To remove a specified RMON history group of statistics, use the **no** form of this command.

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*—(Optional) 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*—(Optional) 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*—(Optional) The number of seconds in each polling cycle. If unspecified, defaults to 1800 (Range: 1–3600).

Command Mode

Interface Configuration mode.

show rmon collection stats

To display the requested RMON history group statistics, use the **show rmon collection stats** Privileged EXEC mode command.

Syntax

show rmon collection stats *[interface-id]*

Parameters

interface-id—(Optional) 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

The following example displays all RMON history group statistics.

```
switchxxxxxx#  show rmon collection stats

Index   Interface   Interval   Requested   Granted   Owner
-----   ---------   --------   Samples     Samples   -------
1       gi1/0/1     30         ---------   -------   CLI
2       gi1/0/1     1800       50          50        Manager
                               50          50
```

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.

show rmon history

To display RMON Ethernet history statistics, use the **show rmon history** Privileged EXEC mode command.

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*—(Optional) Specifies the period of time in seconds to display. (Range: 1–2147483647)

Command Mode

Privileged EXEC mode

Example

The following examples display RMON Ethernet history statistics for index 1:

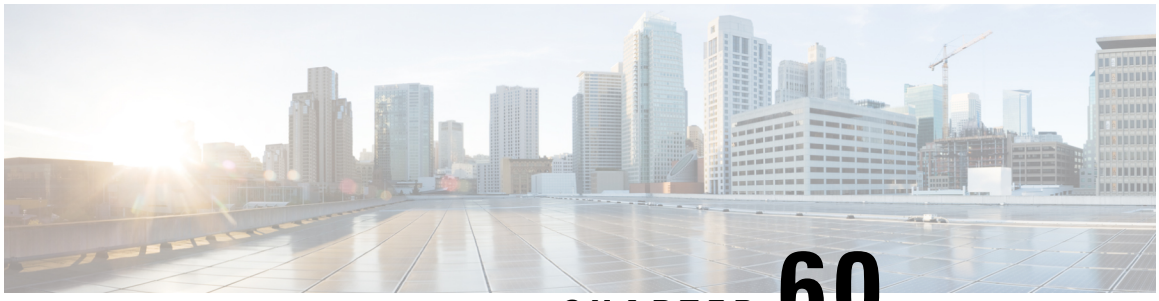
```
switchxxxxxx#  show rmon history 1 throughput
```

```
Sample Set: 1                          Owner: CLI
Interface: gi1/0/1                     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:gi1/0/1                      Interval: 1800
Requested samples: 50                  Granted samples: 50

Maximum table size: 500 (800 after reset)

Time                 CRC Align  Under    Oversize   Fragments  Jabbers
-------------------- ---------- size     ---------- ---------- ----
Jan 18 2005 21:57:00 1          -----    0          49         0
Jan 18 2005 21:57:30 1          1        0          27         0
                                1

switchxxxxxx#  show rmon history 1 other

Sample Set: 1                          Owner: Me
Interface: gi1/0/1                     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.

Field	Description
Utilization	Best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
CRC Align	Number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
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.



CHAPTER 60

Route Map Commands

This chapter contains the following sections:

- match ip address (Policy Routing), on page 961
- match ipv6 address (Policy Routing), on page 962
- route-map (Policy Routing), on page 963
- set ip next-hop, on page 964
- set ipv6 next-hop, on page 965
- show route-map, on page 966

match ip address (Policy Routing)

To match IP packets to perform IP policy routing, use the **match ip address** command in Route Map Configuration Mode. To move the **match ip address** entry, use the **no** form of this command.

Syntax

match ip address access-list *extended-access-list-name*

no match ip address access-list

Parameters

- **access-list** *extended-access-list-name*—Specifies an extended IP ACL.

Default Configuration

No the command is configured.

Command Mode

Route Map Configuration Mode

User Guidelines

The **match ip address** command allows you to policy route IP packets based on criteria that can be matched with an extended IP access list; for example, a protocol, protocol service, and source or destination IP address.

The ACL list specified by the *extended-access-list-name* argument cannot contain the following keywords:

- **time-range**
- **disable-port**
- **log-input**

Example

The example below gives how IPv4 Policy Base Routing is configured:

```
switchxxxxxx(config)# ip access-list extended acl1
switchxxxxxx(config-ip-al)# permit ip 176.212.0.0 00.255.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ip address access-list acl1
switchxxxxxx(config-route-map)# set ip next-hop 173.23.13.20
switchxxxxxx(config-route-map)# exit
```

match ipv6 address (Policy Routing)

To match IPv6 packets to perform IPv6 policy routing, use the **match ipv6 address** command in Route Map Configuration Mode. To move the **match ipv6 address** entry, use the **no** form of this command.

Syntax

match ipv6 address access-list *extended-access-list-name*

no match ipv6 address access-list

Parameters

- **access-list** *extended-access-list-name*—Specifies an extended IPv6 access list.

Default Configuration

No the command is configured.

Command Mode

Route Map Configuration Mode

User Guidelines

The **match ipv6 address** command allows you to policy route IPv6 packets based on criteria that can be matched with an extended access list; for example, a protocol, protocol service, and source or destination IPv6 address.

The ACL list specified by the *extended-access-list-name* argument cannot contain the following keywords:

- **time-range**
- **disable-port**
- **log-input**

Example

The example below gives how IPv4 Policy Base Routing is configured:

```
switchxxxxxx(config)# ipv6 access-list acl1
switchxxxxxx(config-ip-al)# permit ipv6 3211:1297::  ::/32 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ipv6 address access-list acl1
switchxxxxxx(config-route-map)# set ipv6 next-hop 3003:17ac::20
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config-ip-al)# exit
```

route-map (Policy Routing)

To define the conditions for policy routing, use the **route-map** command in Global Configuration mode and the **match** and **set** commands in Route Map Configuration Mode. To delete an entry, use the **no** form of this command.

Syntax

route-map *map-tag* [*sequence-number*]

no route-map *map-tag* [*sequence-number*]

Parameters

- ***map-tag***—A meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.
- ***sequence-number***—Positive integer number that indicates the position a new route map will have in the list of route maps already configured with the same name. If the parameter is used with the **no** form of this command, the position of the route map should be deleted. If the parameter is omitted in the **route-map** command then a value of 10 is applied. If the parameter is omitted in the **no** format then all route maps sharing same map tag name are deleted.

Default Configuration

Conditions for policy routing is not configured.

Command Mode

Global Configuration mode

User Guidelines

Use the **route-map** command to enter route-map configuration mode. The purpose of the **route map** command is to define policy routing.

The **match** commands specify the conditions under which policy routing occurs and the **set** commands specify the routing actions to perform if the criteria enforced by the match commands are met:

- If a outed packet matches to an ACL with the permit action the packet is forwarded by the **set** command (policy based routing).

- If a outed packet matches to an ACL with the deny action the frame is forwarded by the Forwarding table (regular routing).

A route map can have several sections configured by separate **route-map** commands with the same map tag. When a routed packet is checked by a route map the first section which criteria is forced is applied. If there is no matched section the obvious shortest path using the Forwarding Table is applied.

Example 1. The following example gives an example of a route map with one section. TCP packet sent to subnet 156.12.5.0/24 are passed to the next hop 56.1.1.1.

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

Example 2. The following example gives an example of a route map with two sections. TCP packet sent to subnet 156.12.5.0/24 are passed to the next hop 56.1.1.1 and CP packet sent to subnet 156.122.5.0/24 are passed to the next hop 50.1.1.1.

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# ip access-list extended pr-acl2
switchxxxxxx(config-ip-al)# permit tcp any any 156.122.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr 10
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# route-map pbr 20
switchxxxxxx(config-route-map)# match ip address access-list pr-acl2
switchxxxxxx(config-route-map)# set ip next-hop 50.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

set ip next-hop

To specify the IP address of the next hop policy routing, use the **set ip next-hop** command in Route Map Configuration Mode. To delete an entry, use the **no** form of this command.

Syntax

set ip next-hop *next-hop*

no set ip next-hop

Parameters

- ***next-hop***—IPv4 address of the next hop router.

Default Configuration

This command is disabled by default.

Command Mode

Route Map Configuration Mode

User Guidelines

Use the **set ip next-hop** command to set the IP address of the next hop policy routing.

Example

In the following example sets IP address 192.168.30.1 as the next hop IP address:

```
switchxxxxxx(config)# route-map bpr
switchxxxxxx(config-route-map)# match ip address access-list acl
switchxxxxxx(config-route-map)# set ip next-hop 192.168.30.1
switchxxxxxx(config-route-map)# exit
```

set ipv6 next-hop

To specify the IPv6 address of the next hop policy routing, use the **set ipv6 next-hop** command in Route Map Configuration Mode. To delete an entry, use the **no** form of this command.

Syntax

set ipv6 next-hop *next-hop*

no set ipv6 next-hop

Parameters

- ***next-hop***—IPv6 address of the next hop router or outgoing interface ID for a point-to-point outgping interfaces.

Default Configuration

This command is disabled by default.

Command Mode

Route Map Configuration Mode

User Guidelines

Use the **set ip next-hop** command to set the IPv6 address of the next hop policy routing.

Examples

Example 1. In the following example sets IPv76 address **3003:17ac::20** as the next hop IPv6 address:

```
switchxxxxxx(config)# route-map pbr
switchxxxxxx(config-route-map)# match ipv6 address access-list acl1
switchxxxxxx(config-route-map)# set ipv6 next-hop 3003:17ac::20
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config-ip-al)# exit
```

Example 2. In the following example sets interface tunnel1 as the next hop:

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source 132.1.1.1
switchxxxxxx(config-if)# tunnel destination 192.168.30.1
switchxxxxxx(config-if)# tunnel mode ipv6ip
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# route-map bpr
switchxxxxxx(config-route-map)# match ipv6 address access-list acl
switchxxxxxx(config-route-map)# set ipv6 next-hop tunnel 1
switchxxxxxx(config-route-map)# exit
```

show route-map

To display route maps, use the **show route-map** command in Privileged EXEC mode.

Syntax

show route-map [*map-name*]

Parameters

- ***map-name***—Name of a specific route map.

Default Configuration

Command Mode

Privileged EXEC mode

User Guidelines

Use the **show route-map** *map-name* command, to display one given route map.

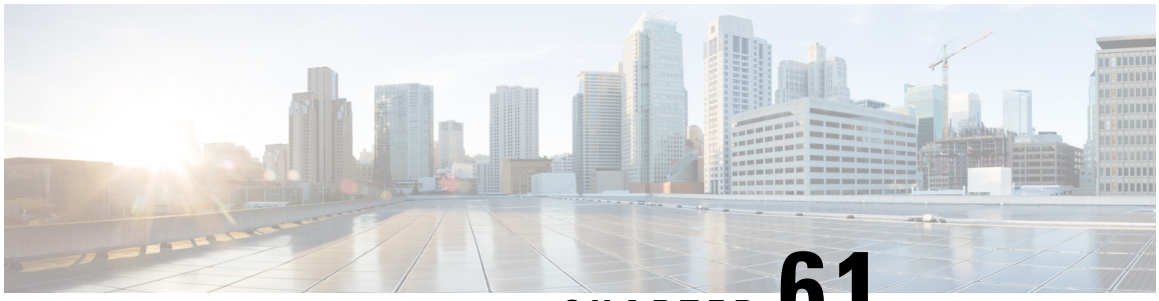
Use the **show route-map** command, to display all configured route maps.

Example

The following is sample output from the show route-map command:

```
switchxxxxxx# show route-map
route-map POLICY-ROUTING, permit, sequence 10
  Match clauses:
    ip address access-lists: acl1
  Set clauses:
    ip next-hop: 192.12.34.5
route-map POLICY-ROUTING, permit, sequence 20
```

```
  Match clauses:
    ip address access-lists: acl2
  Set clauses:
    ip next-hop: 192.122.23.15
route-map POLICY-ROUTING-IPv6, permit, sequence 10
  Match clauses:
    ipv6 address access-lists: acl3
  Set clauses:
    ipv6 next-hop: 3003:17ac::20
route-map POLICY-ROUTING-IPv6, permit, sequence 20
  Match clauses:
    ipv6 address access-lists: acl4
  Set clauses:
    interface next-hop: tunnel 1
```



CHAPTER 61

Router Resources Commands

This chapter contains the following sections:

- set router hardware-routing active, on page 969
- show router hardware-routing status, on page 970
- show system resources, on page 970
- system resources, on page 972

set router hardware-routing active

To start the process of re-activating hardware based routing on the device, use the **set router hardware-routing active** Privileged EXEC mode command.

Syntax

set router hardware-routing active

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

Hardware based routing is supported automatically on device once IPv4 or IPv6 route is enabled. However, hardware based routing is de-activated automatically by the software in cases where device hardware resources cannot support the amount of IPv4 and/or IPv6 entries.

IPv4 entries - IPv4 interfaces/addresses and routes and as well as IPv4 Multicast entries;

IPv6 entries - IPv6 interfaces/addresses and routes as well as IPv6 Multicast entries;

Once Hardware based routing is de-activated by the system the user needs to apply the **set router hardware-routing active** command to re-activate hardware based routing on device. It is recommended to adjust the number of IPv4 and/or IPv6 entries on device to match the device hardware capabilities

Once command is applied, the device begins to update all existing IP entries to device hardware tables. If process succeeds - hardware based routing will be re-activated. If process fails (for example device hardware resource are still not sufficient to support current device IP entries), hardware routing status will remain in-active.

Syslog messages will indicate to user the start of the hardware table update process and the success or failure of such update.

Example 1. The following example the process of reactivating hardware based routing is applied.

```
switchxxxxxx# set router hardware-routing active
This operation may take a few moments...
```

Example 2. In the following example, command is applied, but hardware based routing is already active on the device.

```
switchxxxxxx# set router hardware-routing active
Hardware based routing aleady active
```

show router hardware-routing status

To display the status of hardware based routing, use the **show router hardware-routing status** command in User EXEC mode.

Syntax

show router hardware-routing status

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

Example 1. In the following example, the hardware routing status is displayed as inactive:

```
switchxxxxxx# show system router resources
Hardware routing status: inactive
```

Example 2. In the following example, the hardware routing status is displayed as "in activation" (this will usually indicate that hardware table updated is in process following the activation of command set router hardware-routing active, on page 969):

```
switchxxxxxx# show system router resources
Hardware routing status: in activation
```

show system resources

To display the currently used and max allowed entries for IP Entries, policy based routes and VLAN mapping , use the **show system resources** command in User EXEC mode.

Syntax

show system resources

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

User Guidelines

Use the **show system resources** command to display the currently used and the maximum allowed IP Entries, policy based routes and VLAN mapping entries.

The count of the "in use" entries in command output is calculated as follows:

"*policy routes*" entries - a single entry is consume per each created policy map

- "*vlan mapping*" entries - 8 entries are reserved for system use, and in addition:
  - A single entry is consumed for each VLAN mapping entry applied to an interface
- *"IP entries*" entries - the ip entry count can include different type of entries. The following table details the number of ip entries consume per each entry type::

Logical Entity	Number of IP entries consumed
IP host/Neighbor	1 entry per neighbor
IPv4 interface	2 entries per interface
IPv4 (Remote) Route	1 entries per route
IPv4 Multicast Group	2 entries per group
IPv6 host/Neighbor	4 entries per neighbor
IPv6 interface	8 entries per interface
IPv6 On Link Prefix	4 entries per Prefix
IPv6 (Remote) Route	4 entries per route
IPv6 Multicast Group	8 entries per group

Example

In the following example, per each type, the in use and max entries are displayed:

```
switchxxxxxx# show system resources
                        In-Use              Max
                        ------             --------
IP Entries                 10                 500
IPv4 policy Routes         0                  16
```

```
IPv6 policy Routes          16                32
VLAN Mapping Entries        48                64
```

system resources

To configure hardware resource allocation for policy based routing and/or VLAN mapping , use the **system resources** command in Global Configuration mode. To return to the default, use the **no** form of this command.

Syntax

system resources [**policy-ip-routes** max-number] [**policy-ipv6-routes** max-number] [**vlan-mapping-entries** max-number]

no system resources

Parameters

- **policy-ip-routes** max-number —(Optional) The maximum number of IPv4 policy routes that can be configured. (range: 0- 32)
- **policy-ipv6-routes** max-number —(Optional) The maximum number of IPv6 policy routes that can be configured. (range: 12- 32)
- **vlan-mapping-entries** max-number —(Optional) The maximum number of VLAN Mappings entries that can be configure. (range: 0- 228)

Default Configuration

- policy-ip-routes— 12.
- policy-ipv6-routes— 12.
- vlan-mapping-entries — 0.

Command Mode

Global Configuration mode

User Guidelines

Use the **system resources** command to enter new settings for the maximum supported number of policy based routes and/or VLAN mapping entries. After entering the command, the current setting will be displayed, and the user will be required to confirm saving the new setting to the startup-configuration, following which system needs to be rebooted to apply changes.

When this command is included in a configuration file that is downloaded to the device, if it is downloaded to the running configuration file, the command will be rejected. If it is downloaded to the startup configuration file, the device will not reboot automatically. The new settings will be used after the device is rebooted manually.

Allocating additional resources for policy based routes and/or VLAN mapping entries, means that there are less resources to be used by IP type entries.

Out of the entries allocated for VLAN Mapping - 8 entries are reserved for system use, and cannot be used for user based VLAN Mapping configuration.

Data Validation:

If the new policy based route and/or VLAN mapping values cannot be supported by device (due to relevant resource being used by other applications), the command is rejected and a message is displayed to the user.

If the new max-number parameter is lower than the actual number of entries currently in-use settings, a confirmation message is displayed to the user (before the save confirmation message).

Use the **no system resources** command to restore the default settings.

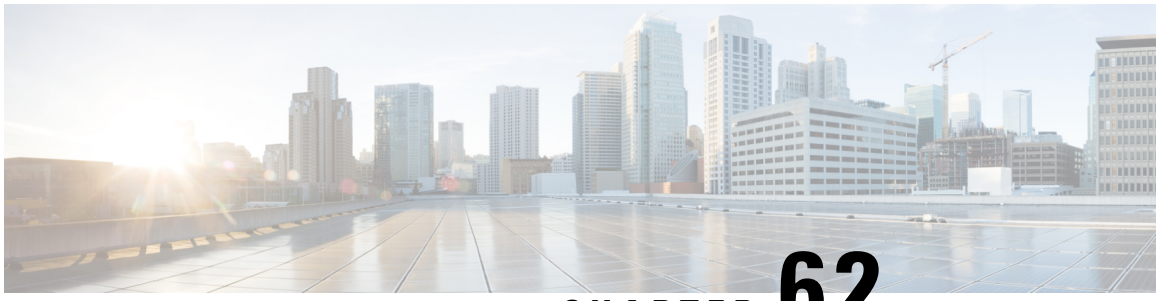
Examples

Example 1 - The following example defines the supported number of entries for IPv4 policy based routes,IPv6 policy based routes and/or VLAN mapping.

```
switchxxxxxx(config)# system resources policy-ip-routes 20 policy-ipv6-routes 32
vlan-mapping-entries 100
                            In-Use  Reserved (Current)  Reserved (New)
                            ------  ------------------  --------------
IPv4 policy Routes              8             16                  20
IPv6 policy Routes              8             16                  32
VLAN Mapping Entries             32            32                  100
Setting the new configuration of entries requires saving the running-configuration file to
 startup-configuration file and rebooting the system, do you want to continue? (Y/N) [N] Y
```

Example 2 - In the following example, the configured entries are less than the entries which are currently in use by the device. Using this configurations means that the system may not have enough resources for the running again in the existing network:

```
switchxxxxxx(config)# system resources policy-ip-routes 8 policy-ipv6-routes 8
vlan-mapping-routes 16
                             In-Use   Reserved (Current)  Reserved (New)
                             ------   ------------------  --------------
IPv4 policy Routes             10             20                    8
IPv6 policy Routes             10              32                   8
VLAN Mapping Entries             50            100                    16
1) In one or more of the parameters, the new max entry configuration is less than the entries
 which are currently in use by the system, do you want to continue?

2) Setting the new configuration of entries requires saving the running-configuration file
 to startup-configuration file and rebooting the system.
Do you want to continue?
Do you want to continue? (Y/N) [N] Y
```



CHAPTER 62

RSA and Certificate Commands

This chapter contains the following sections:

Keys and Certificates

Note DSA keys are not supported when the device is in FIPS compliant mode. Therefore, when in FIPS compliant mode:

- Executing commands based on a DSA key will fail.
- The default DSA keys and certificates are not generated.

Note FIPS 140-2 Compliance is supported on firmware version 4.1.6.x and above.

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

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

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.

The following table describes when these keys/certificates are displayed.

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)

File Type Being Displayed	What is Displayed in a Show Command Without Detailed	What is Displayed in a Show Command With Detailed
Text-based CLI (local backup 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,

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

Destination File Type	Copy from Running Config.	Copy from Startup Config.	Copy from Remote/Local Backup 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 (*.**).
Running Config.	N/A	Only user defines	All keys/certificates present in this file are copied (*).
Text-based CLI (local backup config. file, or remote backup config. file)	All keys (default and user)	Only user defined.	All keys/certificates present in this file are copied.

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

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

- crypto key generate dsa, on page 976
- crypto key generate rsa, on page 977
- crypto key import, on page 978
- show crypto key, on page 979
- crypto certificate generate, on page 980
- crypto certificate request, on page 981
- crypto certificate import, on page 982
- show crypto certificate, on page 986
- show crypto certificate chain, on page 987

crypto key generate dsa

The **crypto key generate dsa** Global Configuration mode command generates a DSA key pair for SSH Public-Key authentication.

Syntax

crypto key generate dsa

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

The size of the created DSA key is 1024 bits

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.

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

This command is not saved in the Running configuration file. However, the keys generated by this command are saved to the Running Configuration file.

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.
.........
```

crypto key generate rsa

The **crypto key generate rsa** Global Configuration mode command generates RSA key pairs for SSH Public-Key Authentication.

Syntax

crypto key generate rsa

Default Configuration

The application creates a default key automatically.

Command Mode

Global Configuration mode

User Guidelines

The size of the created RSA key is 2048 bits

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

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

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

This command is not saved in the Running configuration file. However, the keys generated by this command are saved to the Running Configuration file.

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)#
```

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}

encrypted crypto key import {dsa| rsa}

no crypto key {**dsa| rsa**}

Default Configuration

DSA and RSA key pairs do not exist.

Command Mode

Global Configuration mode

User Guidelines

The imported key must follow the format defined in RFC 4716

DSA key size for import is between 512 bits and 1024 bits

RSA key size for import is between 1024 bits and 2048 bits

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 key 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.

When using the **encrypted** key-word, the private key is imported in its encrypted form.

Example

```
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
switchxxxxxx(config)# 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 ----
```

show crypto key

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

Syntax

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

Parameters

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

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
```

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 rsa** *length*—Regenerates SSL RSA key and specifies the key length.(Supported lengths: 2048 (bits) or 3092 (bits))

  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: 30–1095)

Default Configuration

If the **key-generate** parameter is not used the certificate is generated using the existing key.

The default SSL's RSA key length is 2048.

The default SSL's EC key length is 256.

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 730 days.

Command Mode

Global Configuration mode

User Guidelines

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

If both certificates 1 and 2 have been generated, use the **ip https certificate** command 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 key length is 2048 bytes.

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

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 cerificate generate** command to generate the keys. The certificate fields must be re-entered.

After receiving the certificate from the Certification Authority, use the **crypto cerificate import** 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-----
```

crypto certificate import

The **crypto certificate import** Global Configuration mode command imports a certificate signed by a Certification Authority for HTTPS. In addition, the relevant 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**

encrypted crypto certificate *number* **import**

no crypto certificate *number*

Parameters

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

Command Mode

Global Configuration mode

User Guidelines

Certificate needs to be imported from PEM encoding/file extension

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 cerificate request** command.

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

This command is saved in the Running configuration file.

When using the encrypted form of the command, only the private key must be in encrypted format.

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

```
switchxxxxxx(config)# 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+CYQ2Iarl+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
```

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)
- **mycertificate**—Specifies that only the certificate will be displayed

Default Configuration

displays both keys.

Command Mode

Privileged EXEC mode

Examples

The following example displays SSL certificate # 1 present on the device and the key-pair.

```
switchxxxxxx# show crypto certificate 1
Certificate 1:
Certificate Source: Default
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

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

show crypto certificate chain

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

Syntax

show crypto certificate chain [*number*]

Parameters

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

Default Configuration

Displays both keys.

Command Mode

Privileged EXEC mode

Examples

The following example displays certificate 1 chain:

switchxxxxxx# show crypto certificate chain 1

Certificate Chain - server certificate 1 (Active)

==========

Sever Certificate

Status: valid

Serial Number:

00:16:c9:af:00:2c:7b:06:11:5b:39:3e:de:c4:04:d4:63:11:22:11

Issuer: cn=Intermediate 2 CA, ou=issDept, o=MyInterCA, st=NA, c=US

Subject: cn= momo.company.com, ou=Depd, o=myCompany, st=NA, c=US

Validity:

Not Before: Nov 14 21:06:28 2023 EST

Not After: Nov 09 21:06:28 2043 SET

Intermediate CA Certificate – Inter2

Status: valid

Serial Number: 55:16:c9:af:00:2c:7b:06:11:5b:39:3e:de:c4:04:d4:63:11:22:55

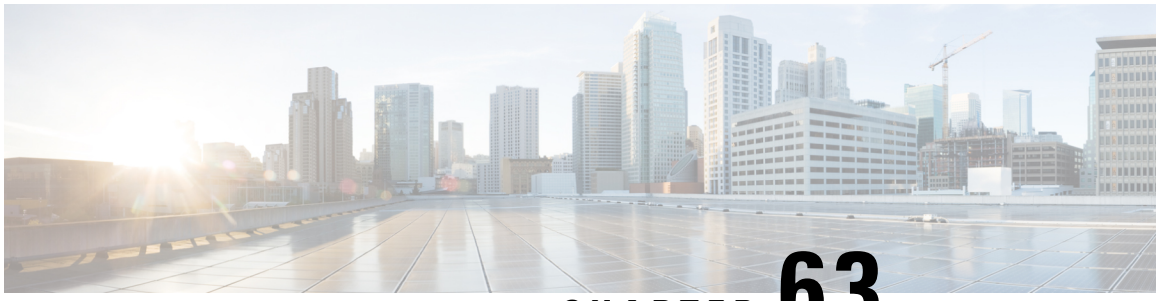
Issuer: cn= My Root CA, ou=RootIss, o=MyRootCA, st=NA, c=US

Subject: cn= Intermediate 2 CA, ou=issDept, o=MyInterCA, st=NA, c=US

Validity:

Not Before: Nov 14 21:06:28 2023 EST

Not After: Nov 09 21:06:28 2043 EST



CHAPTER 63

sFlow Commands

This chapter contains the following sections:

- sflow receiver, on page 989
- sflow flow-sampling, on page 990
- sflow counters-sampling, on page 991
- clear sflow statistics, on page 991
- show sflow configuration, on page 992
- show sflow statistics, on page 992
- sflow receiver source-interface, on page 993
- sflow receiver source-interface-ipv6, on page 994

sflow receiver

To define the sFlow collector, use the **sflow receiver** Global Configuration mode command. To remove the definition of the collector, use the **no** form of this command.

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**—IPv4 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.
- **port**—(Optional) Port number for sflow messages. If unspecified, the port number defaults to 6343. The range is 1-65535.
- **bytes**—(Optional) 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.

sflow flow-sampling

To enable sFlow Flow sampling and configure the average sampling rate of a specific port, use the **sflow flow-sampling** Interface Configuration mode command. To disable Flow sampling, use the **no** form of this command.

Syntax

sflow flow-sampling *rate receiver-index [max-header-size bytes]*

no sflow flow-sampling

Parameters

rate—Specifies the average sampling rate. The sampling rate is calculated as 1/**rate** (Range: 1024–1073741823.)

receiver-index—Index of the receiver/collector (Range: 1–8.)

max-header-size bytes—(Optional) 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 mode

User Guidelines

Configures the sampling rate on the interface. The sampling rate is calculated as 1/rate (the value specified in the command).

Up to 3 rates can be configured on the device. The same rate can be configured on multiple interfaces and is considered a single rate. If more than 3 rates are configured then command will be rejected.

sFlow sampling cannot be enabled on an interface configured as a monitor session source interface.

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).

sflow counters-sampling

To enable sFlow Counters sampling and to configure the maximum interval of a specific port, use the **sflow counters-sampling** Interface Configuration mode command . To disable sFlow Counters sampling, use the **no** form of this command.

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: 15–86400.)

receiver-index—Index of the receiver/collector. (Range: 1–8.)

Default

Disabled

Command Mode

Interface Configuration mode

clear sflow statistics

To clear sFlow statistics, use the **clear sFlow statistics** Privileged EXEC mode command.

Syntax

clear sflow statistics *[interface-id]*

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged 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.

show sflow configuration

To display the sFlow configuration for ports that are enabled for Flow sampling or Counters sampling, use the **show sflow configuration** Privileged EXEC mode command.

Syntax

show sflow configuration *[interface-id]*

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#  show sflow configuration
sFlow Agent Address 172.16.1.1
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
----- -----------     --------- ---------   ---------- -----   ------------
gi1/0/1   1/2048     60 sec    128         1                  1
gi1/0/2   1/4096     Disabled  128         0                  2
Global values
--------------
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

show sflow statistics

To display the sFlow statistics for ports that are enabled for Flow sampling or Counters sampling, use the **show sflow statistics** Privileged EXEC mode command.

Syntax

show sflow statistics *[interface-id]*

Parameters

interface-id—(Optional) Specifies an interface ID. The interface ID must be an Ethernet port.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx#  show sflow statistics
Total sFlow datagrams sent to collectors: 100
```

Interface	Packets sampled	Datagrams sent to collector
---	---	---
gi1/0/1	30	50
gi1/0/2	30	50
gi1/0/3	30	50

sflow receiver source-interface

Use the **sflow receiver source-interface** Global Configuration mode command to specify the source interface whose IPv4 address will be used as the Source IPv4 address for communication with sFlow receivers. Use the **no** form of this command to restore the default configuration.

Syntax

sflow receiver source-interface *interface-id*

no sflow receiver source-interface

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 sFlow server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sflow receiver source-interface vlan 100
```

sflow receiver source-interface-ipv6

Use the **sflow receiver source-interface-ipv6** Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 sFlow receivers. Use the **no** form of this command to restore the default configuration.

Syntax

sflow receiver source-interface-ipv6 *interface-id*

no sflow receiver source-interface-ipv6

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

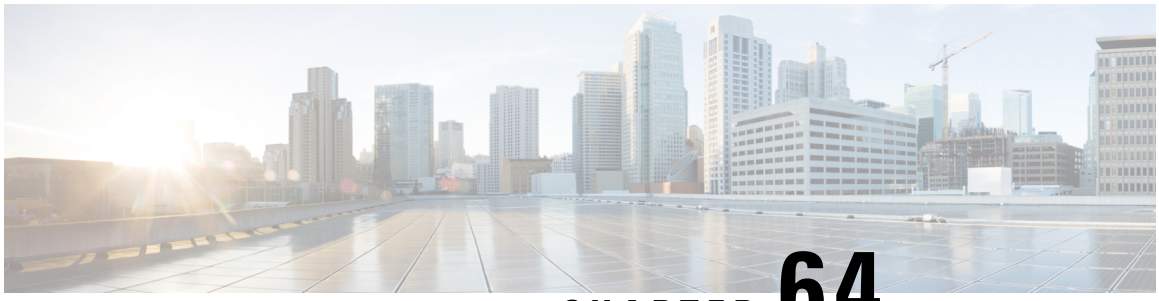
If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 sFlow receiver.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# sflow receiver source-interface-ipv6 vlan 100
```



CHAPTER 64

Smartport Commands

This chapter contains the following sections:

- macro auto (Global), on page 995
- macro auto built-in parameters, on page 996
- macro auto persistent, on page 997
- macro auto processing cdp, on page 998
- macro auto processing lldp, on page 999
- macro auto processing type, on page 999
- macro auto resume, on page 1000
- macro auto smartport (Interface), on page 1001
- macro auto smartport type, on page 1001
- macro auto trunk refresh, on page 1002
- macro auto user smartport macro, on page 1003
- show macro auto ports, on page 1004
- show macro auto processing, on page 1006
- show macro auto smart-macros, on page 1007
- smartport storm-control, on page 1008

macro auto (Global)

The **macro auto** Global Configuration mode command sets the Auto Smartports administrative global state. The **no** format of the command returns to the default.

Syntax

macro auto {enabled | disabled | controlled}

no macro auto

Parameters

- **enabled**—Auto Smartport administrative global and operational states are enabled.
- **disabled**—Auto Smartport administrative global and operational states are disabled.
- **controlled**—Auto Smartport administrative global and operational states are enabled when Auto Voice VLAN is in operation.

Default Configuration

Administrative state is **Disabled**

Command Mode

Global Configuration mode

User Guidelines

Regardless of the status of Auto Smartport, you can always manually apply a Smartport macro to its associated Smartport type. A Smartport macro is either a built-in macro or a user-defined macro. You can define and apply a macro using the CLI commands presented in the Macro Commands section.

If the Auto Smartport Administrative state is controlled, the Auto Smartport Operational state is managed by the Voice VLAN manager and is set as follows:

- Auto Smartport Operational state is disabled when the OUI Voice VLAN is enabled.

  Auto Smartport Operational state is enabled when the Auto Voice VLAN is enabled.

A user cannot enable Auto Smartport globally if the OUI Voice VLAN is enabled.

Example

This example shows an attempt to enable the Auto Smartport feature globally in the controlled mode. This is not possible because the OUI voice feature is enabled. The voice VLAN state is then disabled, after which Auto Smartports can be enabled. The appropriate VLANs are automatically enabled because the ports are configured for Auto Smartports on these VLANs.

```
switchxxxxxx(config)# macro auto controlled
switchxxxxxx(config)# macro auto enabled
Auto smartports cannot be enabled because OUI voice is enabled.
switchxxxxxx(config)# voice vlan state disabled
switchxxxxxx(config)# macro auto enabled
switchxxxxxx(config)#
10-Apr-2011 16:11:31 %LINK-I-Up:  Vlan 20
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 5
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 6
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 7
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 8
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 9
10-Apr-2011 16:11:33 %LINK-I-Up:  Vlan 10
```

macro auto built-in parameters

The **macro auto built-in parameters** Global Configuration mode command replaces the default Auto Smartport values of built-in Smartport macros. The **no** format of the command returns to the default values.

Syntax

macro auto built-in parameters *smartport-type* [*parameter-name value* [*parameter-name value* [*parameter-name value*]]]

no macro auto built-in parameters *smartport-type*

Parameters

- ***smartport-type***—Smartport type (range: **printer**, **desktop**, **guest**, **server**, **host, ip_camera**, i**p_phone**, **ip_phone_desktop**, **switch**, **router** or wireless access point (**ap**)).
- ***parameter-name value***—Specifies the parameter name and its value. These are the parameters of the built-in or user-defined macro defined in the **macro auto user smartport macro** command

Default Configuration

The default value of parameter $native_vlan of the built-in Smartport macros is 1.

For other parameters, the default value is the parameter's default value. For instance, if the parameter is the native VLAN, the default value is the default native VLAN.

Command Mode

Global Configuration mode

User Guidelines

By default, each Smartport type is associated with a pair of built-in macros: a macro that applies the configuration and the anti macro (no macro) to remove the configuration. The Smartport types are the same as the name of the corresponding built-in Smartport macros, with the anti macro prefixed with **no_**.

The value of the parameter **$voice_vlan** cannot be changed by this command.

Example

To change the parameters of a built-in macro:

```
switchxxxxxx(config)# macro auto built-in parameters switch $native_vlan 2
```

macro auto persistent

The **macro auto persistent** Interface Configuration mode command sets the interface as a Smartport persistent interface. The **no** format of the command returns it to default.

Syntax

macro auto persistent

no macro auto persistent

Parameters

This command has no parameters or keywords.

Default Configuration

Persistent is set.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

A Smartport's persistent interface retains its dynamic configuration in the following cases: link down/up, the attaching device ages out, and reboot. Note that for persistence and the Smartport configuration to be effective across reboot, the Running Configuration file must be saved to the Startup Configuration file.

Example

The example establishes two port ranges and makes one persistent and the other not.

```
switchxxxxxx(config)# interface range gi1/0/1-2
switchxxxxxx(config-if-range)# macro auto persistent
switchxxxxxx(config-if-range)# exit
switchxxxxxx(config)# interface range gi1/0/3-4
switchxxxxxx(config-if-range)# no macro auto persistent
```

macro auto processing cdp

The **macro auto processing cdp** Global Configuration mode command enables using CDP capability information to identify the type of an attached device.

When Auto Smartport is enabled on an interface and this command is run, the switch automatically applies the corresponding Smartport type to the interface based on the CDP capabilities advertised by the attaching device(s).

The **no** format of the command disables the feature.

Syntax

macro auto processing cdp

no macro auto processing cdp

Parameters

This command has no parameters or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

To enable CDP globally:

```
switchxxxxxx(config)# macro auto processing cdp
```

macro auto processing lldp

The **macro auto processing lldp** Global Configuration mode command enables using the LLDP capability information to identify the type of an attached device.

When Auto Smartport is enabled on an interface and this command is run, the switch automatically applies the corresponding Smartport type to the interface based on the LLDP capabilities advertised by the attaching device(s).

The **no** format of the command disables the feature.

Syntax

macro auto processing lldp

no macro auto processing lldp

Parameters

This command has no parameters or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

To enable LLDP globally:

```
switchxxxxxx(config)# macro auto processing lldp
```

macro auto processing type

The **macro auto processing type** Global Configuration mode command enables or disables automatic detection of devices of given type. The no format of the command returns to the default.

Syntax

macro auto processing type *smartport-type* {**enabled** | **disabled**}

no macro auto processing type *smartport-type*

Parameters

- ***smartport-type***—Smartport type (range: **host**, i**p_phone**, **ip_phone_desktop**, **switch**, **router** or wireless access point (**ap**)).

Default Configuration

By default, auto detection of ip_phone, ip_phone_desktop, switch, and wireless access point (ap) is enabled.

Command Mode

Global Configuration mode

Example

In this example, automatic detection of wireless access points (ap) is enabled.

```
switchxxxxxx(config)# macro auto processing type ?
  host                set type to host
  ip_phone            set type to ip_phone
  ip_phone_desktop    set type to ip_phone_desktop
  switch              set type to switch
  router              set type to router
  ap                  set type to access point
switchxxxxxx(config)# macro auto processing type ap enabled
```

macro auto resume

The **macro auto resume** Interface Configuration mode command changes the Smartport type from **unknown** to **default** and resumes the Smartport feature on a given interface (but does not reapply the Smartport macro; this is done by the **macro auto trunk refresh** command).

Syntax

macro auto resume

Parameters

This command has no parameters or keywords.

Default Configuration

None

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When a Smartport macro fails at an interface, the Smartport type of the interface becomes **Unknown**. You must diagnose the reason for the failure on the interface and/or Smartport macro, and correct the error.

Example

Changes the Smartport type from **unknown** to **default** and resumes the Smartport feature on port 1.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto resume
```

macro auto smartport (Interface)

The **macro auto smartport** Interface Configuration mode command enables the Auto Smartport feature on a given interface. The **no** format of the command disables the feature on the interface.

Syntax

macro auto smartport

no macro auto smartport

Parameters

This command has no parameters or keywords.

Default Configuration

Enabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

This command is effective only when Auto Smartport is globally enabled.

Example

Enables the Auto Smartport feature on port 1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto smartport
```

macro auto smartport type

The **macro auto smartport type** Interface Configuration mode command manually (statically) assigns a Smartport type to an interface. The **no** format of the command removes the manually-configured type and returns it to **default**.

Syntax

macro auto smartport type *smartport-type* [*parameter-name value* [*parameter-name value* [*parameter-name value*]]]

no macro auto smartport type

Parameters

- ***smartport-type***—Smartport type.

- ***parameter-name value*** —Specifies the parameter name and its value (Range: printer, desktop, guest, server, host, ip_camera, ip_phone, ip_phone_desktop, switch, router or wireless access point (ap)).

Default Configuration

parameter-name *value*—Parameter default value. For instance, if the parameter is the voice VLAN, the default value is the default voice VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

A static type set by the command cannot be changed by a dynamic type.

Example

This example shows an attempt to set the Smartport type of port 1 to printer (statically). The macro fails at line 10.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto smartport type printer
30-May-2011 15:02:45 %AUTOSMARTPORT-E-FAILEDMACRO: Macro printer for auto smar
port type Printer on interface gi1/0/1 failed at command number 10
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# do show parser macro name printer
Macro name : printer
Macro type : default interface
  1. #macro description printer
  2. #macro keywords $native_vlan
  3. #
  4. #macro key description:  $native_vlan: The untag VLAN which will be configu
red on the port
  5. #Default Values are
  6. #$native_vlan = Default VLAN
  7. #
  8. #the port type cannot be detected automatically
  9. #
 10. switchport mode access
 11. switchport access vlan $native_vlan
 12. #
 13. #single host
 14. port security max 1
 15. port security mode max-addresses
 16. port security discard trap 60
 17. #
 18. smartport storm-control broadcast level 10
 19. smartport storm-control include-multicast
 20. smartport storm-control broadcast enable
switchxxxxxx(config)#
```

macro auto trunk refresh

The **macro auto trunk refresh** Global Configuration command reapplies the Smartport macro on a specific interface, or to all the interfaces with the specified Smartport type.

Syntax

macro auto trunk refresh [*smartport-type*] [*interface-id*]

Parameters

- ***smartport-type***—Smartport type (**switch**, **router**, wireless access point (**ap**))
- ***interface-id***—Interface Identifier (port or port channel).

Default Configuration

See User Guidelines.

Command Mode

Global Configuration mode

User Guidelines

The **macro auto smartport** command becomes effective only when the Auto Smartport is globally enabled.

If both *smartport-type* and *interface-id* are defined, the attached Smartport macro is executed on the interface if it has the given Smartport type.

If only *smartport-type* is defined, the attached Smartport macro is executed on all interfaces having the given Smartport type.

If only *interface-id* is defined then the corresponding attached Smartport macro is executed if the interface has one of the following Smartport types: **switch**, **router** or wireless access point **(ap)**.

If a Smartport macro contains configuration commands that are no longer current on one or more interfaces, you can update their configuration by reapplying the Smartport macro on the interfaces.

Example

Adds the ports of Smartport type **switch** to all existing VLANs by running the associated Smartport macros.

```
switchxxxxxx(config)# macro auto trunk refresh switch
```

macro auto user smartport macro

The **macro auto user smartport macro** Global Configuration mode command links user-defined Smartport macros to a Smartport type. This is done by replacing the link to the built-in macro with the link to the user-defined macro. The **no** format of the command returns the link to the default built-in Smartport macro.

Syntax

macro auto user smartport macro *smartport-type user-defined-macro-name* [*parameter-name value* [*parameter-name value* [*parameter-name value*]]]

no macro auto user smartport macro *smartport-type*

Parameters

- ***smartport-type***—Smartport type (range: **printer**, **desktop**, **guest**, **server**, **host**, i**p_camera**, **ip_phone**, **ip_phone_desktop**, **switch**, **router** or wireless access point (**ap**)).
- ***user-defined-macro-name***—Specifies the user-defined macro name that replaces the built-in Smartport macro.
- ***parameter-name*** *value*—Specifies the parameter name and its value in the user-defined macro.

Default Configuration

parameter-name *value*—Parameter's default value. For instance, if the parameter is the native VLAN, the default value is the default native VLAN.

Command Mode

Global Configuration mode

User Guidelines

The scope of each parameter is the macro in which it is defined, with the exception of the parameter **$voice_vlan**, which is a global parameter and its value is specified by the switch and cannot be defined in a macro.

The macros must be defined before linking them in this command.

Smartport macros must be disconnected from the Smartport type before removing them (using the **no** version of this command).

To associate a Smartport type with a user-defined macros, you must have defined a pair of macros: one to apply the configuration, and the other (anti macro) to remove the configuration. The macros are paired by their name. The name of the anti macro is the concatenation of **no_** with the name of the corresponding macro. Please refer to the Macro Command section for details about defining macro.

Example

To link the user-defined macro: my_ip_phone_desktop to the Smartport type: ip_phone_desktop and provide values for its two parameters:

```
switchxxxxxx(config)# macro auto user smartport macro ip_phone_desktop my_ip_phone_desktop
 $p1 1 $p2 2
```

show macro auto ports

The **show macro auto ports** EXEC mode command displays information about all Smartport ports or a specific one. If a macro was run on the port and it failed, the type of the port is displayed as Unknown.

Syntax

show macro auto ports [*interface-id* | **detailed**]

Parameters

- ***interface-id***—Interface Identifier (Ethernet interface, port channel)
- **detailed**—Displays information for non-present ports in addition to present ports.

Default Configuration

Information about all ports is displayed.

Command Mode

User EXEC mode

Examples

Example 1—Note that Smartport on switch and phone types was configured automatically. Smartport on routers was configured statically. Auto smartports are enabled globally.

```
switchxxxxxx# show macro auto ports
Smartport is enabled
Administrative Globally Auto Smartport is enabled
Operational Globally Auto Smartport is enabled
```

Interface	Auto Smartport Admin State	Persistent State	Smartport Type
gi1/0/1	disabled	enabled	router(static)
gi1/0/2	disabled	enabled	switch default
gi1/0/3	enabled	disabled	phone
gi1/0/4	enabled	enabled	

Example 2—Note that Smartport on switch and phone types was configured automatically. Smartport on routers was configured statically. Auto smartports are enabled globally.

```
switchxxxxxx# show macro auto ports
Smartport is enabled
Administrative Globally Auto Smartport is disabled
Operational Globally Auto Smartport is disabled
```

Interface	Auto Smartport Admin State	Persistent State	Smartport Type
gi1/0/1	disabled	enabled	router(static)
gi1/0/2	disabled	enabled	switch default
gi1/0/3	enabled	disabled	phone
gi1/0/4	enabled	enabled	

Example 3—Disabling auto SmartPort on gi1/0/2:

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# no macro auto smartport
switchxxxxxx(config-if)# end
switchxxxxxx# show macro auto ports gi1/0/2
SmartPort is Enabled
Administrative Globally Auto SmartPort is controlled
Operational Globally Auto SmartPort is enabled
```

```
Auto SmartPort is disabled on gi1/0/2
Persistent state is not-persistent
Interface type is default
No macro has been activated
```

Example 4—Enabling auto Smartport on gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# macro auto smartport
switchxxxxxx(config-if)# end
switchxxxxxx# show macro auto ports gi1/0/1
SmartPort is Enabled
Administrative Globally Auto SmartPort is enabled
Operational Globally Auto SmartPort is enabled
Auto SmartPort is enabled on gi1/0/1
Persistent state is persistent
Interface type is switch
Last activated macro is switch
```

show macro auto processing

The **show macro auto processing** EXEC mode command displays information about which protocols (CDP/LLDP) are enabled and which device types can be detected automatically.

Syntax

show macro auto processing

Parameters

This command has no parameters or keywords.

Default Configuration

None

Command Mode

User EXEC mode

Example

```
switchxxxxxx# show macro auto processing
CDB: enabled
LLDP: enabled
host            :disabled
ip_phone        :enabled
ip_phone_desktop:enabled
switch          :enabled
router          :disabled
ap              :enabled
```

show macro auto smart-macros

The **show macro auto smart-macros** EXEC mode command displays the name of Smartport macros, their type (built-in or user-defined) and their parameters. This information is displayed for all Smartport types or for the specified one.

Syntax

show macro auto smart-macros [*smartport-type*]

Parameters

- ***smartport-type***—Smartport type (range: **printer**, **desktop**, **guest**, **server**, **host**, **ip_camera**, i**p_phone**, **ip_phone_desktop**, **switch**, **router** or wireless access point (**ap**)).

Default Configuration

None

Command Mode

User EXEC mode

Example

```
switchxxxxxx# show macro auto smart-macros
SG300-52-R#show macro auto smart-macros
SmartPort type : printer
Parameters     : $native_vlan=1
SmartPort Macro: printer (Built-In)
SmartPort type : desktop
Parameters     : $max_hosts=10 $native_vlan=1
SmartPort Macro: desktop (Built-In)
SmartPort type : guest
Parameters     : $native_vlan=1
SmartPort Macro: guest (Built-In)
SmartPort type : server
Parameters     : $max_hosts=10 $native_vlan=1
SmartPort Macro: server (Built-In)
SmartPort type : host
Parameters     : $max_hosts=10 $native_vlan=1
SmartPort Macro: host (Built-In)
SmartPort type : ip-camera
Parameters     : $native_vlan=1
SmartPort Macro: ip_camera (Built-In)
SmartPort type : ip-phone
Parameters     : $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone (Built-In)
SmartPort type : ip-phone-desktop
Parameters     : $max_hosts=10 $native_vlan=1 $voice_vlan=1
SmartPort Macro: ip_phone_desktop (Built-In)
SmartPort type : switch
Parameters     : $native_vlan=1 $voice_vlan=1
SmartPort Macro: switch (Built-In)
SmartPort type : router
Parameters     : $native_vlan=1 $voice_vlan=1
SmartPort Macro: router (Built-In)
```

```
SmartPort type : ap
Parameters     : $native_vlan=1 $voice_vlan=1
SmartPort Macro: ap (Built-In)
SG300-52-R#
```

smartport storm-control

To enable broadcast, multicast, or unicast storm control on an interface, use the **storm-control** command in Interface (Ethernet, Port Channel) Configuration mode. To return to default, use the **no** form of this command.

Syntax

smartport storm-control broadcast {**level** *level* | **kbps** kbps} [**trap**] [**shutdown**]

no **smartport** storm-control broadcast

smartport storm-control multicast [**registred** | **unregistred**] {**level** *level* | **kbps** *kbps*} [**trap**] [**shutdown**]

no **smartport** storm-control multicast

smartport storm-control unicast {level *level* | kbps *kbps*} [trap] [shutdown]

no **smartport** storm-control unicast

no **smartport** storm-control

Parameters

- **broadcast**—Enables broadcast storm control on the port.
- **multicast** [**registred** | **unregistred**]—Enables ether all multicast, only registered multicast, or only unregistered multicast storm control on the port.
- **unicast**—Enables unicast unknown storm control on the port.
- **level** *level*—Suppression level in percentage. Block the flooding of storm packets when the value specified for level is reached. (Range 1-100)
- **kbps** *kbps*—Maximum of kilobits per second of Broadcast traffic on a port. (Range 1 –10000000)
- **trap**—(Optional) Sends a trap when a storm occurs on a port. If the keyword is not specified the trap is not sent.
- **shutdown**—(Optional) Shut down a port when a storm occurs on the port. If the keyword is not specified extra traffic is discarded.

Default Configuration

Storm control is disabled.

Command Mode

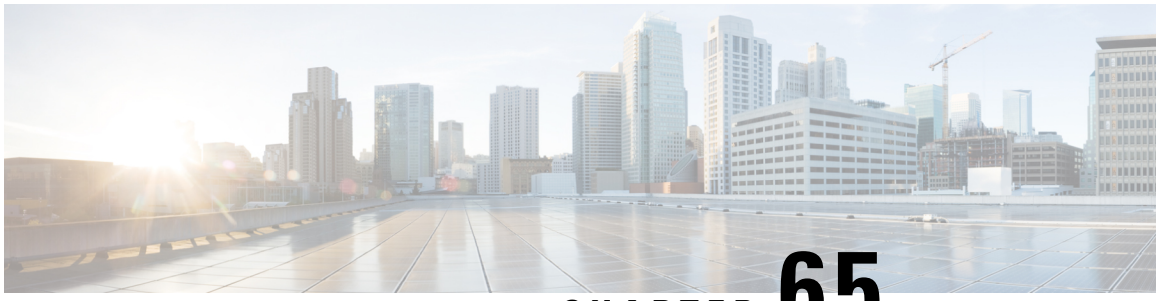
Interface (Ethernet, Port Channel) Configuration mode

Example 1 - Set the maximum number of kilobits per second of Broadcast traffic on port 1 to 10000.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# smartport storm-control broadcast kpbs 10000
```

Example 2 - Set the maximum percentage of kilobits per second of Broadcast traffic on port 1 to 30%.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# smartport storm-control broadcast level 30
```



CHAPTER 65

SNMP Commands

This chapter contains the following sections:

- snmp-server community , on page 1011
- snmp-server community-group, on page 1013
- snmp-server server , on page 1014
- snmp-server source-interface, on page 1014
- snmp-server source-interface-ipv6, on page 1015
- snmp-server view, on page 1016
- snmp-server group, on page 1018
- show snmp views, on page 1019
- show snmp groups, on page 1020
- snmp-server user , on page 1021
- show snmp users, on page 1023
- snmp-server filter, on page 1023
- show snmp filters, on page 1024
- snmp-server host , on page 1025
- snmp-server engineID local, on page 1027
- snmp-server engineID remote , on page 1028
- show snmp engineID, on page 1028
- snmp-server enable traps, on page 1029
- snmp-server trap authentication, on page 1030
- snmp-server contact, on page 1030
- snmp-server location, on page 1031
- snmp-server set, on page 1031
- snmp trap link-status, on page 1032
- show snmp, on page 1032

snmp-server community

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

This command configures both SNMP v1 and v2.

To remove the specified community string, use the **no** form of this command.

Syntax

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

no snmp-server community *community-string [ip-address]* [**type** {**router** | **oob**}]

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- **ro**—(Optional) Specifies read-only access (default)
- **rw**—(Optional) Specifies read-write access
- **su**—(Optional) Specifies SNMP administrator access
- **ip-address**—(Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address.
- **mask**—(Optional) 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**—(Optional) 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.
- **view** *view-name*—(Optional) Specifies the name of a view configured using the command snmp-server view, on page 1016 (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)
- **type** *router*—(Optional) Indicates whether the IP address is on the out-of-band or in-band network.

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, 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
```

snmp-server community-group

To configure access rights to a user group, use **snmp-server community-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]* [**type** {**router** | **oob**}]

Parameters

- **community-string**—Define the password that permits access to the SNMP protocol. (Range: 1–20 characters).
- **group-name**—This is the name of a group configured using snmp-server group, on page 1018 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)
- **ip-address**—(Optional) Management station IP address. The default is all IP addresses. This can be an IPv4 address, IPv6 or IPv6z address.
- **mask**—(Optional) 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**—(Optional) 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.
- **type** *router*—(Optional) Indicates whether the IP address is on the out-of-band or in-band network.

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
```

snmp-server server

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

Syntax

snmp-server server

no snmp-server server

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

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

snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in Global Configuration mode. To returned to the default, use the **no** form of this command.

Syntax

snmp-server source-interface {**traps** | **informs**} *interface-id*

no snmp-server source-interface [**traps** | **informs**]

Parameters

- **traps**—Specifies the SNMP traps interface.
- **informs**—Specifies the SNMP informs.
- **interface-id**—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

If no parameters are specified in **no snmp-server source-interface**, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the **no snmp-server source-interface traps** command to remove the source interface for SNMP traps.

Use the **no snmp-server source-interface informs** command to remove the source interface for SNMP informs.

Use the **no snmp-server source-interface** command to remove the source interface for SNMP traps and informs.

Example

The following example configures the VLAN 10 as the source interface for traps.

```
switchxxxxxx(config)# snmp-server source-interface traps vlan 100
```

snmp-server source-interface-ipv6

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in Global Configuration mode. To returned to the default, use the **no** form of this command.

Syntax

snmp-server source-interface-ipv6 {**traps** | **informs**} *interface-id*

no snmp-server source-interface-ipv6 [**traps** | **informs**]

Parameters

- **traps**—Specifies the SNMP traps interface.
- **informs**—Specifies the SNMP traps informs.
- **interface-id**—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address of the outgoing interface and selected in accordance with RFC6724.

If no parameters are specified in **no snmp-server source-interface**, the default is both traps and informs.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces is selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to send an SNMP trap or inform.

Use the **no snmp-server source-interface-ipv6 traps** command to remove the source IPv6 interface for SNMP traps.

Use the **no snmp-server source-interface-ipv6 informs** command to remove the source IPv6 interface for SNMP informs.

Use the **no snmp-server source-interface-ipv6** command to remove the source IPv6 interface for SNMP traps and informs.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# snmp-server source-interface-ipv6 traps vlan 100
```

snmp-server view

To create or update an SNMP view, use the **snmp-server view** Global Configuration mode command. To remove an SNMP view, use the **no** form of this command.

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)
- **included**—Specifies that the view type is included.
- **excluded**—Specifies that the view type is excluded.
- **oid-tree**—(Optional) 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.

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
```

snmp-server group

To configure an SNMP group, use the **snmp-server group** Global Configuration mode command. Groups are used to map SNMP users to SNMP views. To remove an SNMP group, use the **no** form of this command.

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*—(Optional) Specifies the view name that enables generating informs or a traps. An inform is a trap that requires acknowledgment. Applicable only to the SNMP version 3 security model. (Length: 1–32 characters)
- **read** *readview*—(Optional) Specifies the view name that enables viewing only. (Length: 1–32 characters)
- **write** *writeview*—(Optional) Specifies the view name that enables configuring the agent. (Length: 1–32 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 the snmp-server user , on page 1021 command 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
```

show snmp views

To display SNMP views, use the **show snmp views** Privileged EXEC mode command.

Syntax

show snmp views [*viewname*]

Parameters

viewname—(Optional) 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

show snmp groups

To display the configured SNMP groups, use the **show snmp groups** Privileged EXEC mode command.

Syntax

show snmp groups [*groupname*]

Parameters

groupname—(Optional) 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          V2     no_auth          Default  ""       ""
managers-group      V2     no_auth          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 security. Applicable to SNMP v3 security only .

Field		Description
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.

snmp-server user

To configure a new SNMP user, use the **snmp-server user** Global Configuration mode command. To remove a user, use the **no** form of the command. To enter the authentication and privacy passwords in encrypted form (see SSD), use the **encrypted** form of this command.

Syntax

snmp-server user *username groupname {***v1** | **v2c** | [**remote** *host*] **v3**[**auth** { **sha** | **sha224**| **sha256**| **sha384**| **sha512**} *auth-password* [**priv {aes-128**| **aes-192**| **aes-256}** *priv-password*]]}

encrypted snmp-server user *username groupname {***v1** | **v2c** | [**remote** *host]* **v3**[**auth** { **sha** | **sha224**| **sha256**| **sha384**| **sha512**} *encrypted-auth-password* [**priv** *encrypted-priv-password*]]}

no snmp-server user *username* {**v1** | **v2c** | [**remote** *host*] ***v3***}

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, on page 1018 with v1 or v2c parameters (no specific order of the 2 command configurations is imposed on the user). (Range: Up to 30 characters)
- **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..
- **remote** *host*—(Optional) IP address (IPv4, IPv6 or IPv6z) or host name of the remote SNMP host.
- **auth**—(Optional) Specifies which authentication level is to be used.

  Sha—(Optional) Specifies the HMAC-SHA-96 authentication level.

  Sha224—(Optional) Specifies the HMAC-SHA-224-128 authentication level.

  Sha256—(Optional) Specifies the HMAC-SHA-256-192 authentication level.

  Sha384—(Optional) Specifies the HMAC-SHA-384-256 authentication level.

Sha512—(Optional) Specifies the HMAC-SHA-512-384 authentication level.

- ***auth-password***—(Optional) Specifies the authentication password. Range: Up to 32 characters.
- ***encrypted-auth-password***—(Optional) Specifies the authentication password in encrypted format.
- **priv** *priv-password*—(Optional) specifies private (priv) encryption and the privacy password (Range: Up to 32 characters). The encryption algorithm used is Advanced Encryption Standard (AES) privacy algorithm in Cipher Feedback Mode (CFB) using 128 bits encryption keys),
- ***encrypted-priv-password***—(Optional) Specifies the privacy password in encrypted format.

Default Configuration

No group entry exists.

Command Mode

Global Configuration mode

User Guidelines

For SNMP v1 and v2, this command 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.

A local SNMP EngineID must be defined in order to add SNMPv3 users to the device. For remote hosts users a remote SNMP EngineID is also required.

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 acknowledgment. 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 , on page 1028 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. . User *jerry* is assigned to group *efgh* using SNMP v3.

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user jerry efgh v3 auth sha pass1234
```

show snmp users

To display the configured SNMP users, use the **show snmp users** Privileged EXEC mode command.

Syntax

show snmp users [*username*]

Parameters

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

Default Configuration

Display all users.

Command Mode

Privileged EXEC mode

Example

The following examples displays the configured SNMP users:

```
switchxxxxxx(config)#snmp-server engineid local default
switchxxxxxx(config)# snmp-server group gr1 v3 priv
switchxxxxxx(config)# snmp-server user u1 gr1 v3 auth sha384 sam priv aes-192 xxxx
switchxxxxxx(config)# exit
switchxxxxxx# show snmp users
User name : u1
Group name : gr1
Authentication Method : SHA384
Privacy Method : AES-192
Remote :
Auth Password (Encrypted) : YigwfNcIHMup815E/aM1C8uLBhuKXtO5trhhHSmcGEFQdfTW
o3jrb8PcXl2YK1LS
Priv Password (Encrypted) : f2pSy568NXNoRV9lynTdYjkPQxj26dIc8iE/cNL2Qye8OfqR
1lDVQQCzQ3+0p5Co
```

snmp-server filter

To create or update an SNMP server notification filter, use the **snmp-server filter** Global Configuration mode command. To remove a notification filter, use the **no** form of this command.

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 defined in 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
```

show snmp filters

To display the defined SNMP filters, use the **show snmp filters** Privileged EXEC mode command.

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
```

snmp-server host

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

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.
- **hostname**—Hostname of the host (the targeted recipient). (Range: 1–158 characters. Maximum label size of each part of the host name: 63)
- **trap**—(Optional) Sends SNMP traps to this host (default).
- **informs**—(Optional) Sends SNMP informs to this host. An inform is a trap that requires acknowledgement. Not applicable to SNMPv1.

- ***version* 1**—(Optional) SNMPv1 traps are used.
- ***version* 2c**—(Optional) SNMPv2 traps or informs are used
- ***version* 3**—(Optional) SNMPv2 traps or informs are used
- Authentication options are available for SNMP v3 only. The following options are available:

  noauth—(Optional) Specifies no authentication of a packet.

  auth—(Optional) Specifies authentication of a packet without encryption.

  priv—(Optional) Specifies authentication of a packet with encryption.
- **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 (ISCLI) command for v3.
- **udp-port** *port*—(Optional) UDP port of the host to use. The default is 162. (Range: 1–65535)
- **filter** *filtername*—(Optional) 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*—(Optional) (For informs only) Number of seconds to wait for an acknowledgment before resending informs. The default is 15 seconds. (Range: 1–300)
- **retries** *retries*—(Optional) (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 (ISCLI) 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*

snmp-server engineID local

To specify the SNMP engineID on the local device for SNMP v3, use the **snmp-server engineID local** Global Configuration mode command. To remove this engine ID, use the **no** form of this command.

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 the allocated IANA Enterprise number.
- 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:

- 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
```

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. To remove the configured engine ID, use the **no** form of this command.

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.
- **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.

Example

```
switchxxxxxx(config)# snmp-server engineID remote 1.1.1.1 11:AB:01:CD:23:44
```

show snmp engineID

To display the local SNMP engine ID, use the **show snmp engineID** Privileged EXEC mode command.

Syntax

show snmp engineID

Parameters

This command has no arguments or keywords.

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

snmp-server enable traps

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

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, on page 1030 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
```

snmp-server trap authentication

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

Syntax

snmp-server trap authentication

no snmp-server trap authentication

Parameters

This command has no arguments or keywords.

Default Configuration

SNMP failed authentication traps are enabled.

Command Mode

Global Configuration mode

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
```

snmp-server contact

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

Syntax

snmp-server contact *text*

no snmp-server contact

Parameters

text—Specifies system contact information. (Length: 1–160 characters)

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the system contact information to Technical_Support.

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

snmp-server location

To set the value of the system location string, use the **snmp-server location** Global Configuration mode command. To remove the location string, use the **no** form of this command.

Syntax

snmp-server location *text*

no snmp-server location

Parameters

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

Default Configuration

None

Command Mode

Global Configuration mode

Example

The following example sets the device location to New_York.

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

snmp-server set

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

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.

Example

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

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

snmp trap link-status

To enable link-status generation of SNMP traps, use the **snmp trap link-status** Interface Configuration mode command. To disable generation of link-status SNMP traps, use the **no** form of this command.

Syntax

snmp trap link-status

no snmp trap link-status

Parameters

This command has no arguments or keywords.

Default Configuration

Generation of SNMP link-status traps is enabled

Command Mode

Interface Configuration mode

Example

The following example disables generation of SNMP link-status traps.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# # no snmp trap link-status
```

show snmp

To display the SNMP status, use the **show snmp** Privileged EXEC mode command.

Syntax

show snmp

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example displays the SNMP communications status.

```
switchxxxxxx# show snmp
SNMP is enabled
SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10
SNMP informs Source IPv6 interface:
```

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 Port	Filter Name	TO Sec	Retries
192.122.173.42	Trap	public	2	162		15	3
192.122.173.42	Inform	public	2	162		15	3

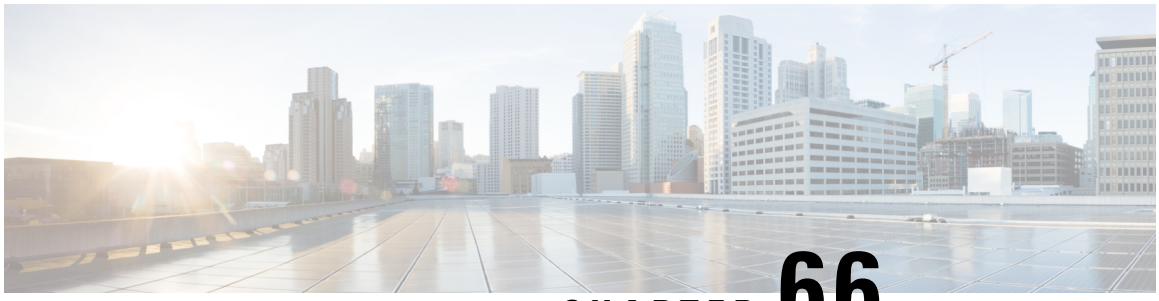
```
Version 3 notifications
```

Target Address	Type	Username	Security Level	UDP Port	Filter name	TO Sec	Retries
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.



CHAPTER 66

SPAN Commands

This chapter contains the following sections:

- monitor session destination, on page 1035
- monitor session source, on page 1037
- remote-span, on page 1039
- show monitor session, on page 1040
- show vlan remote-span, on page 1042

monitor session destination

To create a new Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) destination session, use the **monitor session destination** command in Global Configuration mode. To remove a destination session, use the **no** form of the command.

Syntax

monitor session *session_number* **destination** {{**interface** *interface-id* [**network**]} | {**remote vlan** *vlan-id* **reflector-port** *interface-id*} **network**}

no monitor session *session_number* destination

Parameters

- ***session_number***—Specify the session number identified with the SPAN, RSPAN or flow mirror session. The range is 1 to 4.
- **interface** *interface-id*—Specify the destination interface for the SPAN, RSPAN or flow mirror session (Ethernet port). When the source interface is a RSPAN VLAN the RSPAN VLAN_ID is removed from all frames copied to the interface.
- **network**—Specify that the destination port acts also as a network port.
- **remote vlan** *vlan-id*—Specify the RSPAN VLAN for an RSPAN destination session. Not more than one RSPAN destination VLAN can be defined.
- **reflector-port** *interface-id*—Specify the destination interface for a RSPAN session (Ethernet port). The RSPAN VLAN_ID is added to all frames copied to the interface.

Default Configuration

No SPAN and RSPAN sessions are configured.

Command Mode

Global Configuration mode

User Guidelines

Use the **monitor session** *session_number* **destination interface** *interface-id*, to create a SPAN, local flow mirror, final RSPAN or final remote flow mirror destination session to copy traffic to a destination port.

Use the **monitor session** *session_number* **destination remote vlan** *vlan-id* **reflector-port** *interface-id* command, to create a start RSPAN destination session to copy traffic to a RSPAN VLAN via a reflector port.

A destination or reflector port cannot be a source port.

A destination or reflector port cannot be a OOB port.

If the **network** keyword is not defined only mirrored traffic sent on a destination port and all input traffic is discard and a value of DOWN is advertised as its operational status to all applications running on it.

A destination port configured without the **network** keyword has the following limitations:

- UDLD cannot be enabled on the port.
- 802.1x cannot be enabled on the port.

A port cannot be configured as destination port with the **network** keyword if one the following conditions is true:

- It belongs to the source VLAN
- It belongs to the remote VLAN

Please, do not add the destination port to the source/remote VLAN.

A port cannot be configured as reflector if it belongs to the remote VLAN.

The remote VLAN cannot be configured as a source VLAN.

Only in the final switch the remote VLAN can be configured as a source remote VLAN

A destination port with the **network** keyword or reflector port cannot be configured on an edge port (a port having one of the **vlan-mapping** modes.

Mirrored traffic is sent to queue number 1 of the destination port.

Use the **no monitor session** *session_number* **destination** command to remove one destination session.

Example 1. The following example configures a SPAN session consisting from 3 source and one destination session. The first source session copies traffic for both directions from the source port gi1/0/2, the second source session copies bridges traffic from VLAN 100, and the third source session copies traffic for received on the source port gi1/0/3. The destination session defines port gi1/0/1 as the destination port.

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 source interface gi1/0/3 rx
witchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

Example 2. The following example configures a flow mirror session:

```
switchxxxxxx(config)# ip access-list extended ip1
switchxxxxxx(config-ip-al)# permit ip any any
switchxxxxxx(config-ip-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)# mirror 1
switchxxxxxx(config-pmap-c)# exit
switchxxxxxx(config-pmap)# exit
```

Example 3. The following example configures a RSPAN start session consisting from 2 source and one destination sessions. The first source session copies traffic for both directions from the source port gi1/0/2 and the second session copies traffic from VLAN 100. The destination session defines VLAN 2 as the RSPAN VLAN and port gi1/0/1 as the reflector port.

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
network
```

Example 4. The following example configures a final RSPAN session that copies traffic from a RSPAN VLAN 2 to destination port gi1/0/1:

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote vlan 2
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

monitor session source

To create a new Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) source session, use the **monitor session source** command in Global Configuration mode. To remove a source session, use the **no** form of the command.

Syntax

monitor session *session_number* **source** {**interface** *interface-id* [**both** | **rx** | **tx**]} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*}

no monitor session [*session_number*] **source** [{**interface** *interface-id*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*}]

Parameters

- ***session_number***—Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 4.
- **interface** *interface-id*—Specify the source interface for a SPAN or RSPAN session (Ethernet port).
- **both**, **rx**, **tx**—Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.

- **vlan** *vlan-id*—Specify the SPAN source interface as a VLAN ID. In this case only a value of 1 is allowed for the *session_number* argument.
- **remote vlan** *vlan-id*—Specify the source RSPAN source VLAN ID.

Default Configuration

No SPAN and RSPAN sessions are configured.

Command Mode

Global Configuration mode

User Guidelines

Use the **monitor session** *session_number* **source interface** *interface-id* [**both** | **rx** | **tx**] command, to create a SPAN or RSPAN start source session to monitor traffic that enters or leaves a source port.

Use the **monitor session** *session_number* **source vlan** *vlan-id* command, to create a SPAN or start RSPAN source session to monitor traffic that bridged into a source VLAN.

Use the **monitor session** *session_number* **source remote vlan** *vlan-id* command, to create a final RSPAN source session to monitor traffic that passed via a RSPAN VLAN.

A SPAN or RSPAN session consists from up to 8 sources and one destination with the same session number.

Each **monitor session source** command defines one source port or VLAN. Different **monitor session source** commands must define different sources. A new command with the same session number and the same source overrides the previous defined one.

Up to 8 sources can be defined in one session.

If a packet is mirrored by both the port-based ingress mirroring mechanism, and one of the other ingress mirroring mechanisms, the selected session is the one with the higher session number.

All definitions of different source ports for the same source session must be of the same type: SPAN, start RSPAN start, or RSPAN final.

A source port cannot be a destination port.

A source port cannot be the a OOB port.

The source interface in a RSPAN source switch can not be a membership of the remote VLAN.

Use the **no monitor session** *session_number* **source** {**interface** *interface-id*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*} command to remove one source.

Use the **no monitor session** *session_number* **source** command to remove all sources ports of the given source session.

Example 1. The following example configures a SPAN session consisting from 3 source and one destination session. The first source session copies traffic for both directions from the source port gi1/0/2, the second source session copies bridges traffic from VLAN 100, and the third source session copies traffic for received on the source port gi1/0/3. The destination session defines port gi1/0/1 as the destination port.

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
```

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/3 rx
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

Example 2. The following example configures a RSPAN start session consisting from 2 source and one destination sessions. The first source session copies traffic for both directions from the source port gi1/0/2 and the second session copies traffic from VLAN 100. The destination session defines VLAN 2 as the RSPAN VLAN and port gi1/0/1 as the reflector port

```
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 source vlan 100
switchxxxxxx(config)# monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
network
```

Example 3. The following example configures a final RSPAN session that copies traffic from a RSPAN VLAN 2 to destination port gi1/0/1:

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote vlan 2
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

remote-span

To configure a virtual local area network (VLAN) as a RSPAN remote VLAN, use the **remote-span** command in VLAN Configuration mode. To return to default, use the **no** form of this command.

Syntax

remote-span

no remote-span

Parameters

This command has no arguments or keywords.

Default Configuration

A VLAN is not a RSPAN remote VLAN.

Command Mode

VLAN Configuration mode

User Guidelines

Use the **remote-span** command to define a VLAN as a RSPAN remote VLAN.

Only one Remote VLAN can be defined per switch.

The Remote VLAN must be created manually before configuring of the **remote-span** command.

Guest VLAN cannot be configured as a Remote VLAN.

All traffic into a RSPLAN VLAN is tagged and MAC learning is disabled in a RSPAN VLAN.

The **remote-span** command verifies that all ports of the configured VLAN are egress tagged ports and disables MAC learning. The **no remote-span** command resets MAC learning.

Note. The membership of a RSPAN remote VLAN depended where it is defined:

- Source or Start switch—It is recommended that the RSPAN remote VLAN does not have any memberships.
- Intermediate switch—It is recommended to remove the RSPAN remote VLAN from trunk ports not used for passing mirrored traffic to avoid superfluous flooding. Usually, a RSPAN remote VLAN contains two ports.
- Destination or Final switch—The RSPAN remote VLAN should contain memberships on which the mirrored traffic via this VLAN is arrived. The destination interface cannot be a membership of this VLAN.

Example 1. The following example shows how to configure a RSPAN remote VLAN in a source switch:

```
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source interface gi1/0/2 both
switchxxxxxx(config)# monitor session 1 destination remote vlan 2 reflector-port gi1/0/1
```

Example 2. The following example shows how to configure a RSPAN remote VLAN in a final switch:

```
switchxxxxxx(config)# interface gi1/0/3
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed none
switchxxxxxx(config-if)# switchport trunk allowed add 2
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
switchxxxxxx(config)# monitor session 1 source remote vlan 2
switchxxxxxx(config)# monitor session 1 destination interface gi1/0/1
```

Example 3. The following example shows how to configure a RSPAN remote VLAN in an intermediate switch:

```
switchxxxxxx(config)# interface range gi1/0/3,4
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed none
switchxxxxxx(config-if)# switchport trunk allowed add 2
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# vlan 2
switchxxxxxx(config-vlan)# remote-span
switchxxxxxx(config-vlan)# exit
```

show monitor session

To display information about Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch, use the **show monitor** command in User EXEC mode.

Syntax

show monitor session [*session_number*]

Parameters

- *session_number*—Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 4. If the argument is not defined information about all sessions are displayed.

Default Configuration

This command has no default settings.

Command Mode

User EXEC mode

User Guidelines

Use the **show monitor session** *session_number* command to display information about one session.

Use the **show monitor session** command to display information about all sessions

Example 1. The following example displays information about all SPAN sessions defined into the switch:

```
switchxxxxxx> show monitor session
Session 1
  Type: SPAN
  Source: gi1/0/2, rx only
  Source: VLAN 100
  Source: flow mirrow, policy-map: alpha class-maps: ip-http,  ipv6-http
  Destination: gi1/0/1, network port
```

Example 2. The following example displays information about all start RSPAN sessions defined into the switch:

```
switchxxxxxx> show monitor session
Session 1
  Type: RSPAN Start
  Source: gi1/0/3, both
  Source: VLAN 100
  Source: flow mirrow, policy-map: alpha class-maps: ip-http,  ipv6-http
  Destination: RSPAN VLAN 2, reflector-port gi1/0/1, network port
```

Example 3. The following example displays information about all final RSPAN sessions defined into the switch:

```
switchxxxxxx> show monitor session
Session 1
  Type: RSPAN Final
  Source: RSPAN VLAN 10
  Source: RSPAN VLAN 20
  Destination: gi1/0/1
```

Field Definitions:

- **Type**—The type of the session.
- **Source**—A source of the session. The following options are supported:

Source: *interface-id*, *traffic-direction*(rx only,tx only, or both)

```
The Source is an interface.
```

Source: vlan *vlan-id*

```
The Source is a VLAN.
```

Source: remote vlan *vlan-id*

```
The Source is a RSPAN VLAN (in the RSPAN session final switch).
```

Source: flow mirrow, policy-map: *policy-map-name*, class-maps: *class-map-name1*, *class-map-name2*

```
The Source is a flow mirror, only attached policy-names are displayed.
```

- **Destination**—A destination of the session. The following options are supported:

Destination: *interface-id*

```
The Destination is an interface, regular forwarding on the interface is not supported.
```

Destination: *interface-id*, network

```
The Destination is an interface, regular forwarding on the interface is supported.
```

Destination: RSPAN VLAN *vlan-id*, reflector-port *interface-id*

```
The switch is the first switch in the RSPAN session, regular forwarding on the interface
 is not supported.
```

Destination: RSPAN VLAN *vlan-id*, reflector-port *interface-id*, network

```
The switch is the first switch in the RSPAN session, regular forwarding on the interface
 is supported.
```

show vlan remote-span

To display a list of remote Switched Port Analyzer (RSPAN) VLANs, use the **show vlan remote-span** command in User EXEC mode.

Syntax

show vlan remote-span

Parameters

This command has no arguments or keywords

Default Configuration

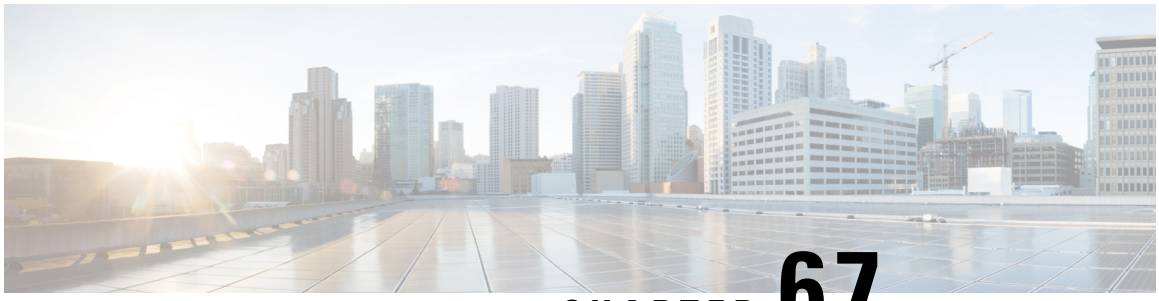
This command has no default settings.

Command Mode

User EXEC mode

Example. This example shows how to display a list of remote SPAN VLANs:

```
switchxxxxxx> show vlan remote-span
Remote SPAN VLAN: 20
```



CHAPTER 67

Spanning Tree Commands

This chapter contains the following sections:

- spanning-tree, on page 1046
- spanning-tree mode, on page 1046
- spanning-tree forward-time, on page 1047
- spanning-tree hello-time, on page 1048
- spanning-tree max-age, on page 1048
- spanning-tree priority, on page 1049
- spanning-tree disable, on page 1050
- spanning-tree cost, on page 1050
- spanning-tree port-priority, on page 1051
- spanning-tree portfast, on page 1052
- spanning-tree link-type, on page 1053
- spanning-tree pathcost method, on page 1053
- spanning-tree bpdu (Global), on page 1054
- spanning-tree bpdu (Interface), on page 1055
- spanning-tree guard root, on page 1056
- spanning-tree bpduguard, on page 1056
- clear spanning-tree counters, on page 1057
- clear spanning-tree detected-protocols, on page 1058
- spanning-tree mst priority, on page 1058
- spanning-tree mst max-hops, on page 1059
- spanning-tree mst port-priority, on page 1060
- spanning-tree mst cost, on page 1060
- spanning-tree mst configuration, on page 1061
- instance (MST), on page 1061
- name (MST), on page 1062
- revision (MST), on page 1063
- show (MST), on page 1063
- exit (MST), on page 1064
- abort (MST), on page 1064
- spanning-tree mst instance, on page 1065
- show spanning-tree, on page 1066
- show spanning-tree bpdu, on page 1077

- spanning-tree loopback-guard, on page 1078
- spanning-tree vlan forward-time, on page 1078
- spanning-tree vlan hello-time, on page 1079
- spanning-tree vlan max-age, on page 1080
- spanning-tree vlan priority, on page 1081
- spanning-tree vlan cost, on page 1082
- spanning-tree vlan port-priority, on page 1082

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

Default Configuration

Spanning-tree is enabled.

Command Mode

Global Configuration mode

Example

The following example enables spanning-tree functionality.

```
switchxxxxxx(config)#  spanning-tree
```

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** | **pvst** | **rapid-pvst**}

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.

- **pvst**—Specifies that the PVST+ is enabled.
- **rapid-pvst**—Specifies that the Rapid PVST+ is enabled.

Default Configuration

The default is RSTP.

Command Mode

Global Configuration mode

User Guidelines

In the RSTP mode, the device uses STP on a port, when the neighbor device uses STP.

In the MSTP mode, the device uses RSTP when the neighbor device uses RSTP, and uses STP when the neighbor device uses STP.

If the PVST mode or the Rapid PVST mode is enabled the switch can support maximum 126 VLANs.

In the Rapid PVST mode, the device uses PVST into a VLAN on a port, when the neighbor device uses PVST.

Examples

The following example enables MSTP.

```
switchxxxxxx(config)#  spanning-tree mode mst
```

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
```

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
```

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
```

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
```

spanning-tree disable

Use the **spanning-tree disable** Interface (Ethernet, Port Channel) Configuration 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

Default Configuration

Spanning tree is enabled on all ports.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables the spanning tree on gi1/0/5

```
switchxxxxxx(config)#  interface gi1/0/5
switchxxxxxx(config-if)#  spanning-tree disable
```

spanning-tree cost

Use the **spanning-tree cost** Interface (Ethernet, Port Channel) Configuration 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	Half the default cost based on Port-channel interface speed	Half the default cost based on Port-channel interface speed
TenGigabit Ethernet (10000 Mbps)	2000	2
5 **Gigabit Ethernet (5000 Mbps)**	12,000	3
2.5 **Gigabit Ethernet (2500 Mbps)**	17,000	4
Gigabit Ethernet (1000 Mbps)	20,000	4
Fast Ethernet (100 Mbps)	200,000	19
Ethernet (10 Mbps)	2,000,000	100

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures the spanning-tree cost on gi1/0/15 to 35000.

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree cost 35000
```

spanning-tree port-priority

Use the **spanning-tree port-priority** Interface (Ethernet, Port Channel) Configuration 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 (Ethernet, Port Channel) Configuration mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the spanning priority on gi1/0/15 to 96

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree port-priority 96
```

spanning-tree portfast

Use the **spanning-tree portfast** Interface (Ethernet, Port Channel) Configuration mode command to enable the PortFast mode. Use the **no** form of this command to disable the PortFast mode.

Syntax

spanning-tree portfast [**auto**]

no spanning-tree portfast

Parameters

- **auto**—Specifies delay before putting the interface into the PortFast mode.

Default Configuration

PortFast mode is set to auto.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

In the PortFast mode, the interface is immediately put into the forwarding state upon linkup, without waiting for the standard forward time delay.

Use the **spanning-tree portfast** command to enable immediately the PortFast mode.

Use the **spanning-tree portfast auto** to delay the PortFast mode for 3 seconds. The interface will turn into the PortFast mode if for this interval it does not receive a Spanning Tree protocol message.

Example

The following example enables the PortFast mode on gi1/0/15.

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree portfast
```

spanning-tree link-type

Use the **spanning-tree link-type** Interface (Ethernet, Port Channel) Configuration 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 (Ethernet, Port Channel) Configuration mode

Example

The following example enables shared spanning-tree on gi1/0/15.

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree link-type shared
```

spanning-tree pathcost method

Use the **spanning-tree pathcost method** Global Configuration mode command to set the default path cost method. Use the **no** form of this command to return to the default configuration.

Syntax

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

Parameters

- **long**—Specifies that the default port path costs are within the range: 1–200,000,000.
- **short**—Specifies that the default port path costs are within the range: 1–65,535.

Default Configuration

Long path cost method.

Command Mode

Global Configuration mode

User Guidelines

This command applies to all the spanning tree instances on the switch.

- If the short method is selected, the switch calculates 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
```

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
```

spanning-tree bpdu (Interface)

Use the **spanning-tree bpdu** Interface (Ethernet, Port Channel) Configuration 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), on page 1054 command determines the default configuration.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example defines the BPDU packet as **flooding** when the spanning tree is disabled on gi1/0/3.

```
switchxxxxxx(config)#  interface gi1/0/3
switchxxxxxx(config-if)#  spanning-tree bpdu flooding
```

spanning-tree guard root

Use the **spanning-tree guard root** Interface (Ethernet, Port Channel) Configuration 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 (Ethernet, Port Channel) Configuration mode

User Guidelines

Root Guard can be enabled when the device operates in any spanning tree mode.

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 gi1/0/1 from being the root port of the device.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  spanning-tree guard root
```

spanning-tree bpduguard

Use the **spanning-tree bpduguard** Interface (Ethernet, Port Channel) Configuration mode command to shut down an interface when it receives a Spanning Tree message. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree bpduguard {**enable** | **disable**}

no spanning-tree bpduguard

Parameters

- **enable**—Enables BPDU Guard.
- **disable**—Disables BPDU Guard.

Default Configuration

BPDU Guard is disabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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 gi1/0/5 when it receives a BPDU.

```
switchxxxxxx(config)#  interface gi1/0/5
switchxxxxxx(config-if)#  spanning-tree bpduguard enable
```

clear spanning-tree counters

Use the **clear spanning-tree counters** Privileged EXEC mode command to clear STP counters on all interfaces or on the specified interface

Syntax

clear spanning-tree counters [**interface** *interface-id*]

Parameters

- ***interface-id***— (O'ptional) 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

The **clear spanning-tree counters** command clears sent and received STP BPDU counters from the entire switch or from the specified interface

Example

This example shows how to clear STP counter on all interfaces.

switchxxxxxx# **clear spanning-tree counters**

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** Privileged EXEC mode 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 the RSTP, MSTP, or Rapid PVST mode.

Example

This restarts the STP migration process on all interfaces.

```
switchxxxxxx#  clear spanning-tree detected-protocols
```

spanning-tree mst priority

Use the **spanning-tree mst priority** Global Configuration mode command to configure the device priority for the specified spanning-tree instance. Use the **no** form of this command to restore the default configuration.

Syntax

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Parameters

- ***instance-id***—Specifies the spanning-tree instance ID. (Range:1– 7 **)**
- ***priority***—Specifies the device priority for the specified spanning-tree instance. This setting determines the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. (Range: 0–61440)

Default Configuration

The default priority is 32768.

Command Mode

Global Configuration mode

User Guidelines

The priority value must be a multiple of 4096.

The switch with the lowest priority is the root of the spanning tree.

Example

The following example configures the spanning tree priority of instance 1 to 4096.

```
switchxxxxxx(config)#  spanning-tree mst 1 priority 4096
```

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

- ***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
```

spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** Interface (Ethernet, Port Channel) Configuration 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– 7 **)**
- ***priority***—Specifies the port priority. (Range: 0–240 in multiples of 16)

Default Configuration

The default port priority is 128.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The priority value must be a multiple of 16.

Example

The following example configures the port priority of gi1/0/1 to 144.

```
switchxxxxxx(config)#  interface gi1/0/1
switchxxxxxx(config-if)#  spanning-tree mst 1 port-priority 144
```

spanning-tree mst cost

Use the **spanning-tree mst cost** Interface (Ethernet, Port Channel) Configuration 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**

Parameters

- ***instance-id***—Specifies the spanning-tree instance ID. (Range:1– 7 **)**

- ***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:

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example configures the MSTP instance 1 path cost for port gi1/0/9 to 4.

```
switchxxxxxx(config)#  interface gi1/0/9
switchxxxxxx(config-if)#  spanning-tree mst 1 cost 4
```

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
```

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– 7**)**
- ***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

Before mapping VLANs to an instance, the instance needs to be created using the spanning-tree mst instance, on page 1065 command (up to 15 instances can be created).

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.

Examples

Example 1. The following example maps VLANs 10-20 to MST instance 1000.

```
switchxxxxxx(config)# spanning-tree mst instance 1000
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1000 vlan 10-20
```

Example 2. In the following example the attempt to map VLANs to MST instance ID 1001 fails, since instance ID 1001 was not created by user:

```
switchxxxxxx(config)# spanning-tree mst configuration
switchxxxxxx(config-mst)# instance 1000 vlan 30-40
Cannot map VLANs to instance 1001. Instance 1001 does not exist.
```

name (MST)

Use the **name** MST Configuration mode command to define the MST region name. Use the **no** form of this command to restore the default setting.

Syntax

name *string*

no name

Parameters

- ***string***—Specifies the MST region 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 region name as Region1.

```
switchxxxxxx(config)#  spanning-tree mst configuration
switchxxxxxx(config-mst)# name region1
```

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
```

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.

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
Digest: 0xB41829F9030A054FB74EF7A8587FF58D
Instance  VLANs Mapped               State
--------  -------------------------  -----
0         1-4094                     Disabled
switchxxxxxx(config-mst)#
```

exit (MST)

Use the **exit** MST Configuration mode command to exit the MST region Configuration mode and apply all configuration changes.

Syntax

exit

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)#
```

abort (MST)

Use the **abort** MST Configuration mode command to exit the MST Configuration mode without applying the configuration changes.

Syntax

abort

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
```

spanning-tree mst instance

Use the spanning-tree mst instance Global Configuration mode command to create an MST instance to which VLANs can be mapped. To delete an instance use the no form of command.

Syntax

spanning-tree mst instance *instance-id*

no spanning-tree mst instance *instance-id*

Parameters

- ***instance-id***—Specifies the spanning-tree instance ID. (range 1-4094)

Default Configuration

Instance IDs 1-4094 do not exist.

Command Mode

Global Configuration mode

User Guidelines

Use the spanning-tree mst instance command to create an MST instance. Up to 15 can be created. Instance 0 (the common and internal spanning tree (CIST) instance) exists by default on device and cannot be removed.

Creating an MST instance allows to map VLANs to this instance in MST Configuration mode) and to configure the following settings on the created instance:

- Configure instance priority - command spanning-tree mst priority, on page 1058.
- Configure port priority per instance - command spanning-tree mst port-priority, on page 1060
- Configure port cost per instance - command spanning-tree mst cost, on page 1060

Use the no form of command to delete an instance. An instance cannot be deleted if one or more VLANs are still mapped to it. Deleting an instance removes all STP configuration related to that instance.

Example

Example 1. The following example creates an MST instance with instance ID of 248:

```
switchxxxxxx(config)#spanning-tree mst instance 248
```

Example 2:The following example removes MST instance 248 from device.

```
switchxxxxxx(config)# no spanning-tree mst instance 248
```

Example 3:In the following example removal of instance ID 365 fails because VLANs are still mapped to this instance:

```
switchxxxxxx(config)# no spanning-tree mst instance 365
Cannot delete instance 365. One or more VLANs are mapped to this instance.
```

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*} | {**vlan** *vlan-id*}]

show spanning-tree [**detail**] [**active** | **blockedports**] [**{instance** *instance-id*} | {**vlan** *vlan-id*}]

show spanning-tree inconsistentports

show spanning-tree mst-configuration

show spanning-tree mst-configuration digest

Parameters

- ***interface-id***—Specifies an interface ID (optional). The interface ID can be one of the following types: Ethernet port or Port-channel.
- **detail**—Displays detailed information.
- **active**—Displays active ports only. Active ports are ports that are STP enabled and in the operational status of up. If device mode is PVST+ or Rapid PVST+ - ports also need to be members of the displayed VLAN.
- **blockedports**—Displays blocked ports only.
- ***instance-id***—MST instance (Range:1– 7**)**. The parameter could be defined only when mode MSTP is enabled.
- **vlan** *vlan-id*—Specifies the VLAN ID. (Range: 1–4094). The parameter could be defined only when mode PVST or RPVST is enabled.
- **inconsistentports** - Displays the ports that are in an inconsistent STP state. Command is relevant only when in PVST+ or Rapid PVST mode.
- **mst-configuration**—Displays the MST configuration information.
- **mst-configuration digest**—Displays the MST configuration digest information.

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:

- **Display examples for a device that is in STP** or RSTP mode -

```
switchxxxxxx#  show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Cost Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 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
gi1/0/1	Enabled	128.1	20000	FRW	Root		P2p (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/3	Disabled	128.3	20000	-	-	No	-
gi1/0/4	Enabled	128.4	20000	BLK	Altn	-	Shared (STP)
gi1/0/5	Enabled	128.5	20000	DIS	-	No -	-

```
switchxxxxxx# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Loopback guard: Disabled
Interfaces
```

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/3	Disabled	128.3	20000	-	-	-	-
gi1/0/4	Enabled	128.4	20000	FRW	Desg	No	Shared (STP)
gi1/0/5	Enabled	128.5	20000	DIS	-	-	-

```
switchxxxxxx#  show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port Hello Time	N/A N/A N/A N/A N/A	Max Age N/A	Forward Delay N/A
Bridge ID	Priority Address	36864 00:02:4b:29:7a:00		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

```
Interfaces
```

Name	State	Prio.Nb	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	-	-	-	-
gi1/0/2	Enabled	128.2	20000	-	-	-	-
gi1/0/3	Disabled	128.3	20000	-	-	-	-
gi1/0/4	Enabled	128.4	20000	-	-	-	-
gi1/0/5	Enabled	128.5	20000	-	-	-	-

```
switchxxxxxx#  show spanning-tree active
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 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
gi1/0/1	Enabled	128.1	20000	FRW	Root	No	P2P (RSTP)
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	Shared (STP)
gi1/0/4	Enabled	128.4	20000	BLK	Altn	No	Shared (STP)

```
switchxxxxxx#  show spanning-tree blockedports
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	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
gi1/0/4	Enabled	128.4	19	BLK	Altn	No	Shared (STP)

```
switchxxxxxx#  show spanning-tree detail
Spanning tree enabled mode RSTP
Default port cost method: long
Loopback guard: Disabled
```

Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 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 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) RSTP Designated bridge Priority: 32768 Designated port id: 128.25 Guard root: Disabled	Role: Root Port cost: 20000 Port Fast: No (configured:no) Address: 00:01:42:97:e0:00 Designated path cost: 0 BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	
Port 2 (gi1/0/2) enabled State: Forwarding Port id: 128.2 Type: Shared (configured: auto) STP Designated bridge Priority: 32768 Designated port id: 128.2 Guard root: Disabled	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000 BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	
Port 3 (gi1/0/3) disabled State: N/A Port id: 128.3 Type: N/A (configured: auto) Designated bridge Priority: N/A Designated port id: N/A Guard root: Disabled	Role: N/A Port cost: 20000 Port Fast: N/A (configured:no) Address: N/A Designated path cost: N/A BPDU guard: Disabled
Number of transitions to forwarding state: N/A BPDU: sent N/A, received N/A	
Port 4 (gi1/0/4) enabled State: Blocking Port id: 128.4 Type: Shared (configured:auto) STP Designated bridge Priority: 28672 Designated port id: 128.25 Guard root: Disabled	Role: Alternate Port cost: 20000 Port Fast: No (configured:no) Address: 00:30:94:41:62:c8 Designated path cost: 20000 BPDU guard: Disabled
Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	
Port 5 (gi1/0/5) enabled State: Disabled Port id: 128.5 Type: N/A (configured: auto) Designated bridge Priority: N/A Designated port id: N/A Guard root: Disabled	Role: N/A Port cost: 20000 Port Fast: N/A (configured:no) Address: N/A Designated path cost: N/A BPDU guard: Disabled

Number of transitions to forwarding state: N/A
BPDU: sent N/A, received N/A
switchxxxxxx# **show spanning-tree ethernet** gi1/0/1

Port 1 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) RSTP Designated bridge Priority: 32768 Designated port id: 128.25 Guard root: Disabled	Role: Root Port cost: 20000 Port Fast: No (configured:no) Address: 00:01:42:97:e0:00 Designated path cost: 0 BPDU guard: Disabled

```
Number of transitions to forwarding state: 1
BPDU: sent 2, received 120638
```

- **Display examples for a device that is in PVST or Rapid PVST mode-**

```
switchxxxxxx#  show spanning-tree
Spanning tree enabled mode Rapid-PVST
Default port cost method: long
Loopback guard: Disabled
VLAN 1
```

Root ID	Priority Address Path Cost Root Port	4096 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 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
gi1/0/1	Enabled	128.1	20000	Frw	Root	No	P2P (RPVST)
gi1/0/2	Enabled	128.2	20000	DSCR	Bkup	No	P2P (RVPST)
gi1/0/3	Disabled	128.3	20000	-	-	No	-
gi1/0/4	Enabled	128.4	20000	Dsbl	Dsbl	No	-
gi1/0/5	Enabled	128.5	20000	DSCR	Altn	Yes	P2P (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

```
* Port Type or PVID Inconsistency
VLAN 20
```

Root ID	Priority Address	4096 00:02:4b:29:7a:00		
	This switch is the root			
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	Dscr*	Desg	No	P2p (RPVST)
gi1/0/3	Disabled	128.3	20000	Dsbl	Dsbl	No	-
gi1/0/4	Enabled	128.4	20000	Dsbl	Dsbl	no	-
gi1/0/5	Enabled	128.5	20000	Dsbl	Dsbl	Yes	P2P (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

```
* Port Type or PVID Inconsistency
switchxxxxxx#  show spanning-tree active
Spanning tree enabled mode Rapid-PVST
Default port cost method: long
Loopback guard: Disabled
VLAN 1
```

Root ID	Priority Address Path Cost Root Port	4096 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
Bridge ID	Priority Address	36864 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
gi1/0/1	Enabled	128.1	20000	Frw	Root	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	DSCR	Bkup	No	P2p (RPVST)
gi1/0/5	Enabled	128.5	20000	DSCR	Altn	Yes	P2p (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

```
* Port Type or PVID Inconsistency
VLAN 20
```

Root ID	Priority Address	4096 00:02:4b:29:7a:00		
	This switch is the root			
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	Dscr*	Desg	Yes	P2p (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

```
* Port Type or PVID Inconsistency
switchxxxxxx#  show spanning-tree VLAN 20
Spanning tree enabled mode PVST
Default port cost method: long
Loopback guard: Disabled
VLAN 20
```

Root ID	Priority Address	4096 00:02:4b:29:7a:00		
	This switch is the root			

	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
gi1/0/1	Enabled	128.1	20000	FRW	Desg	No	P2p (RPVST)
gi1/0/2	Enabled	128.2	20000	Dscr*	Desg	No	P2p (RPVST)
gi1/0/3	Disabled	128.3	20000	Dsbl	Dsbl	No	-
gi1/0/4	Enabled	128.4	20000	Dsbl	Dsbl	no	-
gi1/0/5	Enabled	128.5	20000	Dsbl	Dsbl	Yes	P2P (RPVST)
gi1/0/6	Enabled	128.6	20000	Frw	Desg		Shared(PVST)

* Port Type or PVID Inconsistency

```
switchxxxxxx#  show spanning-tree gi1/0/2
```

VLAN	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
						No	
1	Enabled	128.1	2000	FRW	Root	No	P2p (RPVST)
2	Enabled	128.2	2000	Dscr*	Desg	No	P2p (RPVST)
3	Enabled	128.3	2000	Dscr	Altr	Yes	P2p (RPVST)
6	Enabled	128.6	2000	Frw	Desg		Shared(PVST)

* Port Type or PVID Inconsistency

```
switchxxxxxx#  show spanning-tree gi1/0/2 vlan 3
```

(gi1/0/2) enabled State: Discarding Port id: 128.3 Type: P2p (configured: auto) RPVST Designated bridge Priority: 32768 Designated port id: 128.22 Guard root: Disabled	Role: Alternate Port cost: 2000 Port Fast: No (configured:Auto) Address: 00:01:42:97:e0:00 Designated path cost: 0 BPDU guard: Disabled

```
switchxxxxxx#  show spanning-tree inconsistentports
```

name	interface	inconsistency
VLAN 10	gi1/0/2	Port Type Inconsistency
VLAN 10	gi1/0/7	PVID Inconsistency
VLAN 20	gi1/0/7	PVID Inconsistency
VLAN 20	gi1/0/8	Port Type Inconsistency

Number of inconsistent ports (segments) in the system : 4

- **Display examples for a device that is in MSTP mode -**

```
switchxxxxxx#  show spanning-tree mst-configuration
Name: Region1
Revision: 1
```

Instance	Vlans mapped	State
1	1-9, 21-4094	Enabled
2	10-20	Enabled

```
switchxxxxxx#  show spanning-tree mst-configuration digest
Name: Region1
Revision: 1
Format selector: 0
Digest: 0xB41829F9030A054FB74EF7A8587FF58D
Number of instances configured: 3
switchxxxxxx#  show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
Loopback guard: Disabled
###### MST 0 Vlans Mapped: 1-9
```

CST Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1	
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec
IST Master ID	Priority Address	32768 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
gi1/0/1	Enabled	128.1	20000	FRW	Root	No	P2p Bound
gi1/0/2	Enabled	128.2	20000	FRW	Desg	No	(RSTP)
gi1/0/3	Enabled	128.3	20000	FRW	Desg	No	Shared Bound
gi1/0/4	Enabled	128.4	20000	FRW	Desg	No	(STP)
							P2p
							P2p

```
###### MST 1 Vlans Mapped: 10-20
```

Root ID	Priority Address Path Cost Root Port Rem hops	24576 00:02:4b:29:89:76 20000 gi1/0/4 19
Bridge ID	Priority Address	32768 00:02:4b:29:7a:00

Interfaces

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
gi1/0/1	Enabled	128.1	20000	FRW	Boun	No	P2p Bound
gi1/0/2	Enabled	128.2	20000	FRW	Boun	No	(RSTP)
gi1/0/3	Enabled	128.3	20000	BLK	Altn	No	Shared Bound
gi1/0/4	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
Loopback guard: Disabled
###### MST 0 Vlans Mapped: 1-9
```

CST Root ID	Priority Address Path Cost Root Port	32768 00:01:42:97:e0:00 20000 gi1/0/1		
	Hello Time 2 sec		Max Age 20 sec	Forward Delay 15 sec
IST Master ID	Priority Address	32768 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 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) Boundary RSTP Designated bridge Priority: 32768 Designated port id: 128.25 Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	Role: Root Port cost: 20000 Port Fast: No (configured:no) Address: 00:01:42:97:e0:00 Designated path cost: 0
Port 2 (gi1/0/2) enabled State: Forwarding Port id: 128.2 Type: Shared (configured: auto) Boundary STP Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

Port 3 (gi1/0/3) enabled State: Forwarding Port id: 128.3 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.3 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000
Port 4 (gi1/0/4) enabled State: Forwarding Port id: 128.4 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

MST 1 Vlans Mapped: 10-20

Root ID	Priority Address Path Cost Root Port	24576 00:02:4b:29:89:76 20000 gi1/0/4
	Rem hops 19	
Bridge ID	Priority Address	32768 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 (gi1/0/1) enabled State: Forwarding Port id: 128.1 Type: P2p (configured: auto) Boundary RSTP Designated bridge Priority: 32768 Designated port id: 128.1 Number of transitions to forwarding state: 1 BPDU: sent 2, received 120638	Role: Boundary Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000
Port 2 (gi1/0/2) enabled State: Forwarding Port id: 128.2 Type: Shared (configured: auto) Boundary STP Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

Port 3 (gi1/0/3) disabled State: Blocking Port id: 128.3 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.78 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Alternate Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:1a:19 Designated path cost: 20000
Port 4 (gi1/0/4) enabled State: Forwarding Port id: 128.4 Type: Shared (configured: auto) Internal Designated bridge Priority: 32768 Designated port id: 128.2 Number of transitions to forwarding state: 1 BPDU: sent 2, received 170638	Role: Designated Port cost: 20000 Port Fast: No (configured:no) Address: 00:02:4b:29:7a:00 Designated path cost: 20000

show spanning-tree bpdu

Use the **show spanning-tree bpdu** User 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

User 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 --------- gi1/0/1 gi1/0/2 gi1/0/3	Admin Mode ---------- Filtering Filtering Filtering	Oper Mode --------- Filtering 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 --------- gi1/0/1 gi1/0/2 gi1/0/3	Admin Mode ---------- Global Global Flooding	Oper Mode --------- Flooding STP STP

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

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
```

spanning-tree vlan forward-time

To configure the spanning-tree bridge forward time for a VLAN, use the **spanning-tree vlan forward-time** command in Global Configuration mode. To return to the default settings, use the **no** form of this command.

Syntax

spanning-tree vlan *vlan-range* **forward-time** *seconds*

no spanning-tree vlan *vlan-range* **forward-time**

Parameters

- ***vlan-range***—Specifies a range of VLANs to configure. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 2–4094)
- ***seconds***—Specifies the spanning-tree forward time in seconds. (Range: 4–30)

Default Configuration

The default forward time is 15 seconds.

Command Mode

Global Configuration mode

User Guidelines

The spanning-tree bridge forward time is the amount of time a port remains in the listening and learning states before entering the forwarding state.

When configuring the forwarding time, the following relationship should be maintained:

- 2*(Forward-Time - 1) >= Max-Age

Use this command to configure the forward time for the specified VLAN instance. Setting will take effect if Spanning-tree mode is set to PVST or Rapid PVST .

Example

The following example configures the spanning tree bridge forwarding time to 25 seconds for VLAN 100:

```
switchxxxxxx(config)#  spanning-tree vlan 100 forward-time 25
```

spanning-tree vlan hello-time

To configure the spanning-tree bridge hello time for a VLAN, use the **spanning-tree vlan hello-time** command in Global Configuration mode. To return to the default settings, use the **no** form of this command.

Syntax

spanning-tree vlan *vlan-range* **hello-time** *seconds*

no spanning-tree vlan *vlan-range* **hello-time**

Parameters

- ***vlan-range***—Specifies a range of VLANs to configure. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 2–4094)
- ***seconds***—Specifies the spanning-tree Hello time in seconds. (Range: 1–10)

Default Configuration

The default hello time is 2 seconds.

Command Mode

Global Configuration mode

User Guidelines

The spanning-tree bridge hello time is the time between two sequential sent Hello messages.

When configuring the Hello time, the following relationship should be maintained:

Max-Age >= 2*(Hello-Time + 1)

Use this command to configure the hello time for the specified VLAN instance. Setting will take effect if Spanning-tree mode is set to PVST or Rapid PVST .

Example

The following example configures the spanning-tree bridge hello time to 5 seconds for VLANs 100-101:

```
switchxxxxxx(config)#  spanning-tree vlan 100-101 hello-time 5
```

spanning-tree vlan max-age

To configure the spanning-tree bridge maximum age time for a VLAN, use the **spanning-tree vlan max-age** command in Global Configuration mode. To return to the default settings, use the **no** form of this command.

Syntax

spanning-tree vlan *vlan-range* **max-age** *seconds*

no spanning-tree vlan *vlan-range* **max-age**

Parameters

- ***vlan-range***—Specifies a range of VLANs to configure. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 2–4094)
- ***seconds***—Specifies the spanning-tree bridge maximum age in seconds. (Range: 6–40)

Default Configuration

The default max-age value is 15 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)

Use this command to configure the maximum age for the specified VLAN instance. Setting will take effect if Spanning-tree mode is set to PVST or Rapid PVST .

Example

The following example configures the spanning-tree bridge maximum age to 10 seconds for VLAN 100:

```
switchxxxxxx(config)#  spanning-tree vlan 100 max-age 10
```

spanning-tree vlan priority

To configure the spanning-tree bridge priority for a VLAN, use the **spanning-tree vlan priority** command in Global Configuration mode. To return to the default settings, use the **no** form of this command.

Syntax

spanning-tree vlan *vlan-range* **priority** *priority*

no spanning-tree vlan *vlan-range* **priority**

Parameters

- ***vlan-range***—Specifies a range of VLANs to configure. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 2–4094)
- ***priority***—Specifies the bridge priority. (Range: 0–61440)

Default Configuration

The default priority equal to 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.

Use this command to configure the bridge priority for the specified VLAN instance. Setting will take effect if Spanning-tree mode is set to PVST or Rapid PVST .

Example

The following example configures the spanning-tree priority to 12288 for VLAN 100-105:

```
switchxxxxxx(config)#  spanning-tree vlan 100-105 priority 12288
```

spanning-tree vlan cost

To configure the spanning-tree bridge path cost for a port and a VLAN, use the **spanning-tree vlan cost** command in Interface (Ethernet, Port Channel) Configuration mode. To return to the default settings, use the **no** form of this command.

Syntax

spanning-tree vlan *vlan-range* **cost** *cost*

no spanning-tree vlan *vlan-range* **cost**

Parameters

- ***vlan-range***—Specifies a range of VLANs to configure. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 2–4094)
- ***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).

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use this command to configure the port cost for the specified VLAN instance. Setting will take effect if Spanning-tree mode is set to PVST or Rapid PVST .

The VLAN instances that can be specified are VLAN ID 2-4094.

Example

The following example configures the spanning-tree cost to 35000 for port gi1/0/15 and VLAN 100:

```
switchxxxxxx(config)#  interface gi1/0/15
switchxxxxxx(config-if)#  spanning-tree vlan 100 cost 35000
```

spanning-tree vlan port-priority

To configure the spanning-tree port priority for a VLAN, use the **spanning-tree vlan port-priority** command in Interface (Ethernet, Port Channel) Configuration mode. To return to the default settings, use the **no** form of this command.

Syntax

spanning-tree vlan *vlan-range* **port-priority** *priority*

no spanning-tree vlan *vlan-range* **port-priority**

Parameters

- ***vlan-range***—Specifies a range of VLANs to configure. To specify a range, use a hyphen. To specify a series, use a comma. (Range: 2–4094)
- ***priority***—Specifies the port priority. (Range: 0–240)

Default Configuration

The default port priority is 128.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

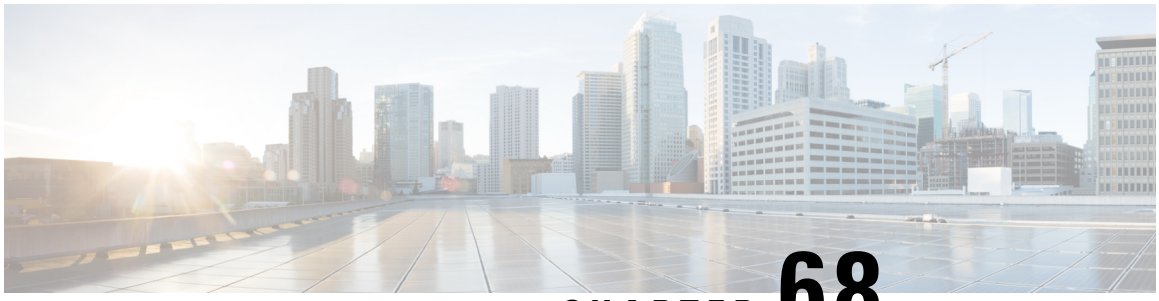
The priority value must be a multiple of 16.

Use this command to configure the port priority for the specified VLAN instance. Setting will take effect if Spanning-tree mode is set to PVST or Rapid PVST .

Example

The following example configures the spanning priority on gi1/0/15 to 16 for VLANs 100-102:

```
switchxxxxxx(config)#  interface gi1/0/15-16
switchxxxxxx(config-if)#  spanning-tree vlan 100-102 port-priority 96
```



CHAPTER 68

SSD Commands

This chapter contains the following sections:

- ssd config, on page 1085
- passphrase, on page 1086
- ssd rule, on page 1087
- show SSD, on page 1088
- ssd session read, on page 1090
- show ssd session, on page 1090
- ssd file passphrase control, on page 1091
- ssd file integrity control, on page 1092

ssd config

To enter the Secure Sensitive Data (SSD) command mode, use **ssd config** in Global Configuration mode. In this command mode, an administrator can configure how the sensitive data on the device, such as keys and passwords, is to be protected.

Syntax

ssd config

Parameters

This command has no arguments or keywords.

Command Mode

Global Configuration mode

User Guidelines

Only users with sufficient permission can use this command, which edits and displays the SSD configuration. See ssd rule, on page 1087 for a description of these permissions.

Example

```
switchxxxxxx(config)# ssd config
switchxxxxxx(config-ssd)#
```

passphrase

To change the passphrase in the system, use **passphrase** in SSD Configuration mode. A device protects its sensitive data by encrypting them using the key generated from the passphrase.

To reset the passphrase to the default passphrase, use the **no passphrase**.

Syntax

passphrase *{passphrase}*

encrypted passphrase *{encrypted-passphrase}*

no passphrase

Parameters

- **passphrase**—New system passphrase.
- **encrypted-passphrase**—The passphrase in its encrypted form.

Default Usage

If this command is not entered, the default passphrase is used.

Command Mode

SSD Configuration mode

User Guidelines

To use this command, enter passphrase and Enter, a confirmation message is displayed and the user must confirm the intention to change the passphrase. Then the passphrase can be entered (see example).

Encrypted passphrase is allowed only in the SSD Control Block of a source file that is being copied to the startup configuration file (user cannot manually enter this command).

When generating a passphrase, the user must use 4 different character classes (similar to strong password/passwords complexity). These can be: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.

Example

The following example defines a decrypted passphrase.

```
switchxxxxxx(config-ssd)# passphrase
This operation will change the system SSD passphrase. Are you sure? (Y/N)[N] Y
Please enter SSD passphrase:**********
Please reenter SSD passphrase:**********
```

ssd rule

To configure an SSD rule, use **ssd rule** in SSD Configuration mode. A device grants read permission of sensitive data to users based on the SSD rules. A user that is granted **Both** or **Plaintext** read permission is also granted permission to enter SSD Configuration mode.

To delete user-defined rules and restore default rules, use **no ssd rule**.

Syntax

[encrypted] SSD rule {***all*** **|** *level-15* **|** *default-user* **|** *user user-name*}

{***secure*** **|** *insecure* | ***secure-xml-snmp*** **|** *insecure-xml-snmp}*

permission {***encrypted-only*** **| plaintext-only | both |** *exclude*}

default*-read* **{***encrypted* | ***plaintext*** **|** *exclude*}

no ssd rule [{***all*** **|** *level-15* **|** *default-user* **|** *user user-name*}

{***secure*** **|** *insecure* | ***secure-xml-snmp*** **|** *insecure-xml-snmp*}]

Command Mode

SSD Configuration mode.

Default Rules

The device has the following factory default rules:

Table 4: Default SSD Rules

Rule Key		Rule Action	
User	**Channel**	**Read Permission**	**Default Read Mode**
level-15	secure-xml-snmp	Plaintext Only	Plaintext
level-15	secure	Both	Encrypted
level-15	insecure	Both	Encrypted
all	insecure-xml-snmp	Exclude	Exclude
all	secure	Encrypted Only	Encrypted
all	insecure	Encrypted Only	Encrypted

User Guidelines

Use **no ssd rule** to delete a user-defined rule or to restore the default of a modified default rule.

Use **no ssd rule** (without parameters) to remove all SSD rules and restore the default SSD rules. A confirmation message will be displayed asking permission to do this. To delete specific rules (applicable for the user defined), provide parameters specifying the user and security of the channel.

encrypted SSD rule is used to copy an SSD rule from one device to another in a secure manner.

You can modify but cannot delete the default SSD rules. The following is the order in which SSD rules are applied:

- The SSD rules for specified *users*.
- The SSD rule for the **default-user (cisco)**.
- The SSD rules for **level-15** users.
- The remaining SSD rules for **all**.

The user can enter the commands in any order.The ordering is done implicitly by the device.

Example 1 - The following example modifies a rule.

```
switchxxxxxx(config-ssd)# ssd rule level-15 secure permission encrypted-only default-read
encrypted
```

Example 2 - The following example adds a rule.

```
switchxxxxxx(config-ssd)# ssd rule user james secure permission both default-read encrypted
```

Example 3 - The following example adds a rule as encrypted format.

```
switchxxxxxx(config-ssd)# encrypted ssd rule iurwe874jho32iu9ufjo32i83232fdefsd
```

Example 4 - The following example deletes a default rule.

```
switchxxxxxx(config-ssd)# no ssd rule all secure
```

Example 5 - The following example deletes a user-defined rule.

```
switchxxxxxx(config-ssd)# no ssd rule user james secure
```

Example 6 - The following example deletes all rules.

```
switchxxxxxx(config-ssd)# no ssd rule
This operation will delete all user-defined rules and retrieve the default rules instead.
Are you sure (Y/N): N
```

show SSD

To present the current SSD rules; the rules will be displayed as plaintext, use **show ssd rules** in SSD Configuration mode.

Syntax

show SSD [***rules*** | ***brief***]

Parameters

- **rules**—(Optional) Display only the SSD rules.
- **brief**—(Optional) Display the encrypted passphrase, File Passphrase Control and File Integrity attributes.

Command Mode

SSD Configuration mode

Default Configuration

Display all SSD information.

Example 1 - The following example displays all SSD information.

```
switchxxxxxx(config-ssd)# show ssd
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
 User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
  Specific    admin11       secure            Both        Encrypted   User-Define
  Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
  Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
  Level-15                  secure            Both        Encrypted     Default
  Level-15                 insecure           Both        Encrypted     Default
    All                     secure       Encrypted-Only   Encrypted     Default
    All                    insecure      Encrypted-Only   Encrypted     Default
    All                insecure-xml-snmp Plaintext-Only   Plaintext    *Default
* Modified default entry
```

Example 2 - The following example displays the SSD rules.

```
switchxxxxxx(config-ssd)# show ssd rules
 User Type   User Name      Channel      Read Permission Default Read    Type
------------ --------- ----------------- --------------- ------------ -----------
  Specific    admin11       secure            Both        Encrypted   User-Define
  Specific    admin2        secure       Encrypted-Only   Encrypted   User-Define
  Level-15              secure-xml-snmp  Plaintext-Only   Plaintext     Default
  Level-15                  secure            Both        Encrypted     Default
  Level-15                 insecure           Both        Encrypted     Default
    All                     secure       Encrypted-Only   Encrypted     Default
    All                    insecure      Encrypted-Only   Encrypted     Default
    All                insecure-xml-snmp Plaintext-Only   Plaintext    *Default
* Modified default entry
```

Example 3 - The following example displays the SSD attributes.

```
switchxxxxxx(config-ssd)# show ssd brief
SSD current parameters:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
SSD parameters after reset:
Local Passphrase:        Default
File Passphrase Control: Unrestricted
File Integrity Control:  Disabled
```

ssd session read

To override the current SSD default read of the current session, use **ssd session read** in Global Configuration mode.

Syntax

ssd session read {***encrypted*** | ***plaintext*** | ***exclude***}

no **ssd session** read

Parameters

- **encrypted**—Override the SSD default option to encrypted
- **plaintext**—Override the SSD default option to plaintext
- **exclude**—Override the SSD default option to exclude

Command Mode

Global Configuration mode.

Default

The command itself does not have a default. However, note that the read mode of the session itself, defaults to the default read mode of the SSD rule that the device uses to grant SSD permission to the user of the session.

User Guidelines

Use **no ssd session read** to restore the default read option of the SSD rules. This configuration will be allowed only if the user of the current session has sufficient read permissions; otherwise, the command will fail and an error will be displayed. The setting will take effect immediately and will terminate when the user restores the settings or exits the session.

Example

```
switchxxxxxx(config)# ssd session read plaintext
```

show ssd session

To view the SSD read permission and default read mode of the user of the current session, use **show ssd session in** Privileged EXEC mode.

Syntax

show ssd session

Command Mode

Privileged EXEC mode

Default

None

Examples

```
switchxxxxxx# show ssd session
User Name/Level: James / Level 15
User Read Permission:  Both
Current Session Read mode: Plaintext
```

ssd file passphrase control

To provide an additional level of protection when copying configuration files to the startup configuration file, use **ssd file passphrase control in** SSD Configuration mode. The passphrase in a configuration file is always encrypted with the default passphrase key

Syntax

ssd file passphrase control {***restricted*** | ***unrestricted***}

no ssd file passphrase control

Parameters

- **Restricted**—In this mode, a device restricts its passphrase from being exported into a configuration file. Restricted mode protects the encrypted sensitive data in a configuration file from devices that do not have the passphrase. The mode should be used when a user does not want to expose the passphrase in a configuration file.
- **Unrestricted**—In this mode, a device will include its passphrase when creating a configuration file. This allows any devices accepting the configuration file to learn the passphrase from the file.

Default

The default is **unrestricted**.

Command Mode

SSD Configuration mode.

User Guidelines

To revert to the default state, use the **no ssd file passphrase control** command.

Note that after a device is reset to the factory default, its local passphrase is set to the default passphrase. As a result, the device will not be able to decrypted sensitive data encrypted with a user-defined passphrase key in its own configuration files until the device is manually configured with the user-passphrase again or the files are created in unrestricted mode.

If a user-defined passphrase in Unrestricted mode are configured, it is highly recommended to enable SSD File Integrity Control. Enabling SSD File Integrity Control protects configuration files from tampering.

Examples

```
console(ssd-config)# ssd file passphrase control restricted
console(ssd-config)# no ssd file passphrase control
```

ssd file integrity control

To instruct the device to protect newly-generated configuration files that contain encrypted sensitive data from tampering, use **ssd file integrity control** command in SSD Configuration mode.

To disable Integrity Control, use **no ssd file integrity control**.

Syntax

ssd file integrity control ***enabled***

no ssd file integrity control

Parameters

- **enabled**—Enable file integrity control to protect newly-generated configuration files from tampering.

Default

The default file input control is **disable**.

Command Mode

SSD Configuration mode.

User Guidelines

TA user can protect a configuration file from being tampered by creating the file with File Integrity Control enabled. It is recommended that File Integrity Control be enabled when a devices users a user-defined passphrase with Unrestricted Configuration File Passphrase Control.

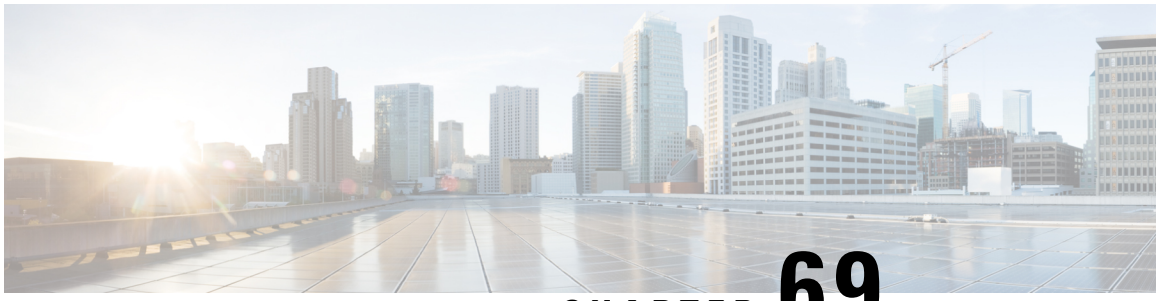
A device determines whether the integrity of a configuration file is protected by examining the File Integrity Control command in the file. If a file in integrity-protected, but a device finds the integrity of the file is not intact, the device rejects the file. Otherwise, the file is accepted for further processing.

Examples

```
switchxxxxxx(config-ssd)#  ssd file integrity control enabled
```

When File Integrity is enabled, an internal digest command is added to the end of the entire configuration file. This is used in downloading the configuration file to the startup configuration.

```
config-file-digest 0AC78001122334400AC780011223344
```



CHAPTER 69

SSH Client Commands

This chapter contains the following sections:



Note DSA keys are not supported when the device is in FIPS compliant mode. Therefore, when in FIPS compliant mode:

- Executing commands based on a DSA key will fail.
- The default DSA keys and certificates are not generated.

- ip ssh-client algorithm, on page 1093
- ip ssh-client authentication, on page 1095
- ip ssh-client change server password, on page 1096
- ip ssh-client key, on page 1097
- ip ssh-client password, on page 1099
- ip ssh-client server authentication, on page 1100
- ip ssh-client server fingerprint, on page 1100
- ip ssh-client source-interface, on page 1101
- ipv6 ssh-client source-interface, on page 1102
- ip ssh-client username, on page 1103
- show ip ssh-client, on page 1104
- show ip ssh-client server, on page 1105

ip ssh-client algorithm

To enable one or more of the alogrithms used by the client for the SSH session encryption, host-key key exchange (kex) or MAC, use the **ip ssh-client algorithm** command in Global Configuration mode. To disable one or more of the SSH alogorithm, use the **no** form of this command.

Syntax

ip ssh-client algorithm {encryption enc-alg1 [enc-alg-2…] | **hostkey** host-alg1[host-alg2…] | **kex** kex-alg1[kex-alg2…] | mac mac-alg1[mac-alg2…]}

no ip ssh-client algorithm {encryption enc-alg1 [enc-alg-2…] | hostkey host-alg1[host-alg2…] | kex kex-alg1[kex-alg2…] | mac mac-alg1[mac-alg2…]}

Parameters

- **encryption** enc-alg1 [enc-alg-2…] (optional) – list of encryption algorithms advertised to the client. One or more of the following algorithms can be specified:
  - **aes128-ctr** - AES with 128-bit key in CTR mod
  - **aes192-ctr** - AES with 192-bit key in CTR mod
  - **aes256-ctr** - AES with 256-bit key in CTR mod
  - **aes128-gcm** - AES with 128-bit key in GCM mode. Compatible with aes128-gcm@openssh.com
  - **aes256-gcm** - AES with 256-bit key in GCM mode. Compatible with aes256-gcm@openssh.com
- **hostkey** host-alg1[host-alg2…] (optional) – list of Host-key public-key algorithms advertised to the client. One or more of the following algorithms can be specified:
  - **ssh-dss** - DSA public-key signature with SHA1 hash
  - **ssh-rsa** - RSA public-key signature with SHA1 hash
  - **rsa-sha2-256** - RSA public-key with SHA2-256 hash
  - **rsa-sha2-512** - RSA public-key with SHA2-512 hash
- **kex** kex-alg1[kex-alg2…] (Optional) – Enable one or more of the following SSH key exchange (kex) algorithms:
  - **diffie-hellman-group16-sha512** - Diffie-Hellman key exchange using SHA2-512 as HASH and 4096-bit MODP Group
  - **diffie-hellman-group14-sha1** - Diffie-Hellman key exchange using SHA1 as HASH and 2048-bit MODP Group
- **mac** mac-alg1[mac-alg2…] (optional) - Enable one or more of the following SSH

  Message Authentication Code (MAC) algorithms:
  - **hmac-sha1** - HMAC-SHA1 (digest length = key length = 160 bits)
  - **hmac-sha2-256** - HMAC-SHA2-256 (digest length = key length = 256 bits)
  - **hmac-sha2-512** - HMAC-SHA2-512 (digest length = key length = 512 bits)

Default Configuration

- Enabled Encryption algorithms: aes128-ctr, aes192-ctr, aes256-ctr, chacha20-poly1305, aes128-gcm and aes256-gcm
- Enabled host-key alogrithms: ssh-dss, ssh-rsa, rsa-sha2-256 and rsa-sha2-512
- Enabled kex algorithms: diffie-hellman-group16-sha512 and diffie-hellman-group14-sha1
- Enabled MAC algorithms: hmac-sha1, hmac-sha2-256 and hmac-sha2-512

Command Mode

Global Configuration mode

User Guidelines

Use the ip ssh-client algorithm command to specify which encryption, host-key, key exchange (kex) and MAC algorithm will be advertised by the SSH client. Algorithms not specified in the command will not be advertised.

The no ip ssh-client algorithm specifies which algorithms to remove from the SSH client advertisement. The no command will change the advertisement list only if it specifies an algorithm that is in the current advertisement list. At least one algorithm must be supported for each category. If the command attempts to remove the last algorithm supported for that category the operation will fail and an error message will be displayed.

The configuration file will include a command that specifies the algorithm that are advertised (even if no ip ssh-client algorithm was used for the configuration)

The following algorithms are supported, and can be disabled only if FIPS mode is disabled:

- chacha20-poly1305 encryption
- ssh-dss host-key

In FIPS enabled mode these algorithms are not supported, and therefore do not need to be disabled.

Examples

Example 1 - The following example enables a few of the SSH encryption algorithms on the device. This means that the other encryption algorithms will not be advertised by the SSH client:

```
Switchxxxxxx(config)# ip ssh-client algorithm encryption aes256-ctr aes256-gcm
```

ip ssh-client authentication

To define the SSH client authentication method used by the local SSH clients to be authenticated by remote SSH servers, use the **ip ssh-client authentication** command in Global Configuration mode.

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 mode

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
```

ip ssh-client change server password

To change a password of an SSH client on a remote SSH server, use the **ip ssh-client change server password** command in Global Configuration mode.

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 ":".

Command Mode

Global Configuration mode

User Guidelines

Use the command to change a password on a remote SSH server. Use the **ip ssh-client password** command 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
```

ip ssh-client key

To create a key pair for SSH client authentication by public key (either by generating a key or by importing a key), use the **ip ssh-client key** command in Global Configuration mode. To remove a key, use the **no** form of the command.

Syntax

ip ssh-client key {**dsa** | **rsa**} {**generate | key-pair** *privkey pubkey***}**

encrypted ip ssh-client key {**dsa** | **rsa**} **key-pair** *encrypted-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.

  encrypted-privkey—private key is in encrypted format.

  pubkey—The plaintext pubic key.

Default Configuration

The application creates a key automatically; this is the default key.

Command Mode

Global Configuration mode

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 5: Keys, Defaults and Users

From/To	Show	Show (detailed)	Copy/Upload of Running Config	Copy/Upload of Startup Config	Download te (TFTP/Backu
Startup Config	Only user-defined	N/A	All keys (default and user)	N/A	All keys (def
Running Config	Keys are not displayed.	All keys (default and user)	N/A	Only user defined.	Same as user
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.

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
```

ip ssh-client password

To configure the password for SSH client authentication by password, use the **ip ssh-client password** command in Global Configuration mode. To return to default, use the **no** form of the command.

Syntax

ip ssh-client password *string*

encrypted ip ssh-client password *encrypted-string*

no ip ssh-client password

Parameters

- ***string***—Password for the SSH clients (1 - 70 characters). The password cannot include the characters "@" and ":".
- ***encrypted-string***—Password for the SSH client in encrypted form.

Default Configuration

The default password is anonymous.

Command Mode

Global Configuration mode

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.

If the **encrypted** keyword is used, the password must be in the encrypted form.

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
```

ip ssh-client server authentication

To enable remote SSH server authentication by the SSH client, use the **ip ssh-client server authentication** command in Global Configuration mode.

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

This command has no arguments or keywords.

Default Configuration

SSH server authentication is disabled

Command Mode

Global Configuration mode

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
```

ip ssh-client server fingerprint

To add a trusted server to the Trusted Remote SSH Server Table, use the **ip ssh-client server fingerprint** command in Global configuration mode. 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 an SSH server.
- ***ip-address***—Specifies the address of an 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 mode

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
```

ip ssh-client source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 SSH servers, use the **ip ssh-client source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

ip ssh-client source-interface *interface-id*

no ip ssh-client **source-interface**

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# ip ssh-client source-interface vlan 100
```

ipv6 ssh-client source-interface

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 SSH servers, use the **ipv6 ssh-client source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

ipv6 ssh-client source-interface *interface-id*

no ipv6 ssh-client **source-interface**

Parameters

- ***interface-id***—(Optional) Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface then the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface then the minimal IPv4 address defined on the source interface and with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SSH servers.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# ipv6 ssh-client source-interface vlan 100
```

ip ssh-client username

To configure the SSH client username of the switch, use the **ip ssh-client username** command in Global Configuration mode.

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 mode

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**

show ip ssh-client

To display the SSH client credentials, both default and user-defined keys, use the **show ip ssh-client** command in Privilege EXEC mode.

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 only 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 1. The following example displays the authentication method and the RSA public key:

```
switchxxxxxx# show ip ssh-client mypubkey rsa
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
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
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
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
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Authentication method:   DSA key
Username:                anonymous (default)
Password:                anonymous (default)
password(Encrypted):     KzGgzpYa7GzCHhaveSJDehGJ6L3Yf9ZBAU5nsxSxwic=
```

show ip ssh-client server

To display the SSH remote server authentication method and the Trusted Remote SSH Server table, use the **show ip ssh-client server** command in Privilege EXEC Configuration mode.

Syntax

show ip ssh-client server [*host* | *ip-address*]

Parameters

- ***host***—(Optional) DNS name of an SSH server.
- ***ip-address***—(Optional) IP Address of an SSH server. The IP address can be an IPv4, IPv6 or IPv6z address. See IPv6z Address Conventions.

Default Configuration

None

Command Mode

Privileged EXEC 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 1 - In the following example, the SSH remote server authentication method and all trusted remote SSH servers are displayed:

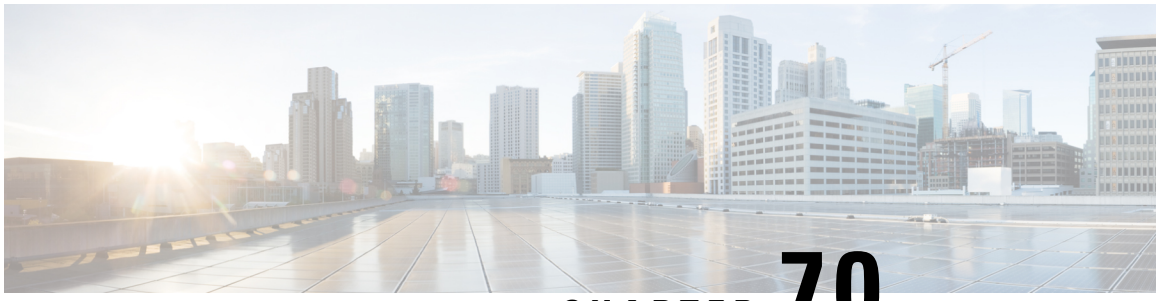
```
switchxxxxxx# show ip ssh-client server
SSH Server Authentication is enabled
server address: 11.1.0.1
  Server Key Fingerprint: 5a:8d:1d:b5:37:a4:16:46:23:59:eb:44:13:b9:33:e9
server address: 192.165.204.111
  Server Key Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
server address: 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
```



CHAPTER 70

Stack Commands

This chapter contains the following sections:

- set stack unit-type, on page 1107
- set stack mode, on page 1108
- stack unit, on page 1109
- stack configuration, on page 1110
- show stack configuration, on page 1111
- show stack, on page 1111
- show stack links, on page 1112

set stack unit-type

To configure the unit type of a stack member , use the **set stack unit-type** Privileged EXEC mode command.

set stack unit-type unit *unit-id* **network** *network-type* **uplink** *uplink-type*

Parameters

- **unit** unit-id - Define the unit ID to apply setting. (Range: 1–**4**)
- **network** network-type - The type of network ports of the unit. Supported values are:
  - gi (for device for which all network ports types are Gigabitethernet)
  - tw (for device for which all network ports types are TwoPointFiveGigabitEthernet).
  - te (for device for which all network ports typs are Tengigabitethernet).
- **uplink** *uplink-type* - The type of uplink ports of the unit. Supported values are:
  - te (for device with Tengigabitethernet uplink ports)
  - none (for devices with no uplink ports)

Default Configuration

User defined type is not configured

Command Mode

Privileged EXEC mode

User Guidelines

Use the **set stack unit-type** command to define the type of "not-present" stack units (see below). The type of unit in stack defines the type of interface naming for this unit and determines which interface level commands can be applied.

If a unit is present or inserted in a stack, the unit type is automatically set by the software to the type of unit identified. If unit that was present is subsequently removed from stack the unit will become "not-present" but retain the existing unit type. If a unit is "not-present", and there is no previous type identified (unit did not exist previously in stack), its unit type is automatically set to the same unit type as the Active unit.

- if **network** port type is set to te, **uplink** port type must be set to none.
- if **network** port type is set to gi or tw , **uplink** port type must be set to te.
- If the command is applied to a unit which is present in stack, command will fail with the following error message: "Unit ID X is present in stack - cannot manually set unit type"
- The unit-type of each unit is saved across reboots and displayed as part of configuration file header in the following format: "**unit-type unit** X **network** *network-type* **uplink** *uplink-type*"

Example 1—The following example sets the unit type of unit 3.

```
switchxxxxxx# set stack unit-type unit 3 network gi uplink te
```

set stack mode

To configure the stack mode of all units in stack after reboot, use the **set stack mode** Privileged EXEC mode command.

Syntax

set stack mode {**native**| **hybrid**}

Parameters

- **native** - all units in stack are of the same type (network interfaces type is the same on all units).
- **hybrid** - units in stack contain units of different types (network interfaces type of different units may be different).

Default Configuration

native mode

Command Mode

Privileged EXEC mode

User Guidelines

- command is applied to all units in stack
- After prompting user, command will reload all devices in stack.
- Reseting stack/unit to factory default will return all units to native mode (the default)
- In case of changing mode from native to hybrid mode, the command will delete stack startup configuration as well, and may upgrade inactive image version on all units to active image version (if current inactive image does not support hybrid mode) . It is advisable to save device configuration to external server before changing modes.

Example 1—The following example sets all units in stack to hybrid mode.

```
switchxxxxxx# set stack mode hybrid
Following confirmation, changing the stacking mode to hybrid will:
* Delete the startup configuration file;
* Upgrade the in-active image to the active image version (in case in-active image version
 does not support hygrid mode);
* Automatically reload the stack;
It is highly recommended that you will backup the configuration before changing the mode,
continue ? (Y/N)[N] Y
```

Example 2—The following example sets all units in stack to native mode.

```
switchxxxxxx# set stack mode native
Changing the stacking mode to native will reload the stack, continue ? (Y/N)[N] Y
```

stack unit

To place the user in the context of the specified stack unit or all stack units, use the **stack unit** Global Configuration command.

Syntax

stack unit {*unit-id* | ***all***}

Parameters

- **unit-id**— Select a specific unit. All commands after this command refer to this unit. Unit must be member in the stack. (Range: 1–**4**).
- ***all*—**Select **all the units in the stack.**

Default Configuration

None

Command Mode

Global Configuration mode

Example 1—The following example sets the unit context to 2, all following stack command will apply to unit 2.

```
switchxxxxxx(config)# stack unit 2
```

Example 2—The following example sets the unit context to all units in the stack, all following stack command will apply to all the units.

```
switchxxxxxx(config)# stack unit all
```

stack configuration

To configure the ports and unit id after reboot, use the **stack configuration** command.

Syntax

stack configuration {[***links*** *ports-list*] [***unit-id*** {*unit-id* | ***auto***}] *}*

no stack configuration

Parameters

- ***links***— Select port list to be used as stack links after reload.
- ***ports-list*** - a list of one or more stack ports separated by comma, or a range of sequential ports marked by dash.

  no-links— set stack unit without stack links after reboot.
- ***unit-id***— Select the unit id to be used after reload. (Range: 1–**4**). Use ***auto*** to enable stack auto numbering feature.

Command Mode

Global Configuration mode

Stack Unit mode.

User Guidelines

- Running the command in Global Configuration mode will configure the current stack Active unit.
- The **no stack configuration** is used to return the stack configuration to factory default after reload (use the **reload** command to reboot unit).
- Running the command in **stack unit** *all* context and configuration of the ***unit-id*** parameter not to ***auto*** generate an error (to avoid setting several units to the same Id)**.**
- Optional parameters not provided in the command will not be changed.

Example 1—The following example sets the Active unit to stack factory default.

```
switchxxxxxx(config)# no stack configuration
```

Example 2—The following example sets the unit 3 to have stack links (ports) te3-4 with unit ID auto.

```
switchxxxxxx(config)# stack unit 3
switchxxxxxxunit# stack configuration links te3-4 unit-id auto
```

show stack configuration

To display the stack configuration (including configuration that is configured after reboot) parameters, use the **show stack configuration** EXEC mode command.

Syntax

show stack configuration

Command Mode

User EXEC mode

Examples

Display the stack configuration information for an entire stack.

```
switchxxxxxx# show stack configuration
```

Unit Id	After Reboot Configuration	
	Unit Id	Stack Links
----------	----------	----------
1	1	te1-2
2	auto	te3-4
3	4	te1-2

show stack

To display the stack operational status, use the **show stack** EXEC mode command.

Syntax

show stack

Command Mode

User EXEC mode

Examples

Display the stack information for an entire stack.

```
switchxxxxxx# show stack
Topology is Ring
Units stack mode: Hybrid
```

Unit Id	MAC Address	Role	Network Port Type	Uplink Port Type
-------	------------------	---------	--------	---------
1	00:00:b0:00:10:00	Active	te	none
2	00:00:b0:00:20:00	Standby	gi	te
3	00:00:b0:00:30:00	Member	gi	te
4	00:00:b0:00:40:00	Member	tw	te

show stack links

To display the stack links operational status, use the **show stack links** EXEC mode command.

Syntax

show stack links [details]

Command Mode

User EXEC mode

Example 1—Display the stack links information for an entire stack.

```
switchxxxxxx# show stack links
```

Topology is Ring

Unit Id	Active Links	Neighbor Links	Operational Link Speed	Down/Standby Links
----------	----------	----------	----------	----------
1	te1/1-2	te3/4,te2/1	10G	te1/3,te1/4
2	te2/1-2	te1/2,te3/3	10G	
3	te3/3-4	te2/2,te1/1	10G	

Example 2—Display the stack links information for an entire stack with details.

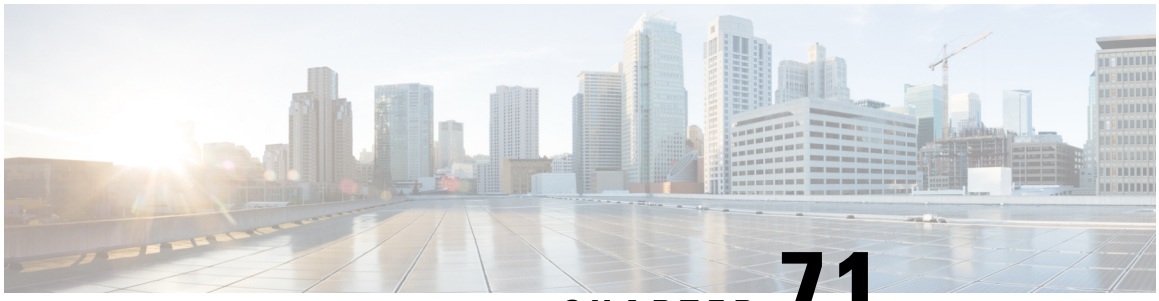
.

```
switchxxxxxx# show stack links details
```

Unit Id	Link	Status	Speed	Neighbor Unit Id	Neighbor Link	Neighbor Mac Address
----------	----------	----------	----------	----------	----------	----------

Unit Id	Link	Status	Speed	Neighbor Unit Id	Neighbor Link	Neighbor Mac Address
1	te1	Active	10G	2	te2	00:00:b0:00:20:00
1	te2	Down	NA	NA	NA	NA
2	te1	Down	NA	NA	NA	NA
2	te2	Active	10G	1	te1	00:00:b0:00:10:00

Topology is Ring



CHAPTER 71

SYSLOG Commands

This chapter contains the following sections:

- aaa logging, on page 1115
- clear logging, on page 1116
- clear logging file, on page 1117
- file-system logging, on page 1117
- logging buffered, on page 1118
- logging console, on page 1119
- logging file, on page 1119
- logging file threshold percent, on page 1120
- logging host , on page 1120
- logging on, on page 1121
- logging source-interface, on page 1122
- logging source-interface-ipv6, on page 1123
- logging aggregation on, on page 1124
- logging aggregation aging-time, on page 1124
- logging origin-id, on page 1125
- logging cbd module, on page 1125
- logging cbd level, on page 1126
- show logging, on page 1127
- show logging file, on page 1128
- show syslog-servers, on page 1128

aaa logging

To enable logging AAA logins, use the **aaa logging** Global Configuration mode command. To disable logging AAA logins, use the **no** form of this command.

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
```

clear logging

To clear messages from the internal logging buffer, use the **clear logging** Privileged EXEC mode command.

Syntax

clear logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the internal logging buffer.

```
switchxxxxxx# clear logging
Clear Logging Buffer ? (Y/N)[N]
```

clear logging file

To clear messages from the logging file, use the **clear logging file** Privileged EXEC mode command.

Syntax

clear logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

Command Mode

Privileged EXEC mode

Example

The following example clears messages from the logging file.

```
switchxxxxxx# clear logging file
Clear Logging File [y/n]
```

file-system logging

To enable logging file system events, use the **file-system logging** Global Configuration mode command. To disable logging file system events, use the **no** form of this command.

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
```

logging buffered

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 **logging buffered** Global Configuration mode command. To cancel displaying the SYSLOG messages, and to return the buffer size to default, use the **no** form of this command.

Syntax

logging buffered [*buffer-size*] [*severity-level* | *severity-level-name*]

no logging buffered

Parameters

- **buffer-size**—(Optional) Specifies the maximum number of messages stored in buffer. (Range: 20–1000)
- **severity-level**—(Optional) Specifies the severity level of messages logged in the buffer. The possible values are: 1-7.
- **severity-level-name**—(Optional) 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 1000.

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 and severity level **informational**.

```
switchxxxxxx(config)# logging buffered debugging
switchxxxxxx(config)# logging buffered 100 informational
```

logging console

To limit messages logged to the console to messages to a specific severity level, use the **logging console** Global Configuration mode command. To restore the default, use the **no** form of this command.

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
```

logging file

To limit SYSLOG messages sent to the logging file to messages with a specific severity level, use the **logging file** Global Configuration mode command. To cancel sending messages to the file, use the **no** form of this command.

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
```

logging file threshold percent

To enable the logging file usage alarm, and to configure the alarm threshold, use the logging file threshold Global Configuration mode command. To disable the logging file usage alarm, use the no form of this command.

Syntax

logging file threshold *percent*

no logging file threshold

Parameters

percent —Specifies the alarm threshold in percents (range 1-99).

Default Configuration

Logging file usage alarm is disabled.

Command Mode

Global Configuration mode

User Guidelines

Use the logging file threshold command to enable logging file usage alarm and to set the threshold at which the alarm will be generated. Once the logging file capacity passes the defined threshold a syslog message will be generated to indicate the logging file passed the defined threshold. Using the no form of the command will disable the logging file threshold alarm.

Example

The following example defines 50% as the threshold for the logging file.

```
switchxxxxxx(config)# logging file threshold 50
```

logging host

To log messages to the specified SYSLOG server, use the **logging host** Global Configuration command. To delete the SYSLOG server with the specified address from the list of SYSLOG servers, use the **no** form of this command.

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.
- **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*—(Optional) Port number for SYSLOG messages. If unspecified, the port number defaults to 514. (Range: 1–65535)
- ***severity*** *level*—(Optional) Limits the logging of messages to the SYSLOG servers to a specified level: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, Debugging.
- ***facility*** *facility*—(Optional) 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*—(Optional) 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
```

logging on

To enable message logging, use the **logging on** Global Configuration mode command. This command sends debug or error messages asynchronously to designated locations. To disable the logging, use the **no** form of this command.

Syntax

logging on

no logging on

Parameters

This command has no arguments or keywords.

Default Configuration

Message logging is enabled.

Command Mode

Global Configuration mode

Example

The following example enables logging error messages.

```
switchxxxxxx(config)# logging on
```

logging source-interface

To specify the source interface whose IPv4 address will be used as the source IPv4 address for communication with IPv4 SYSLOG servers, use the **logging source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

logging source-interface *interface-id*

no logging source-interface

Parameters

interface-id—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to the next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the lowest IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 SYSLOG server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface vlan 100
```

logging source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 SYSLOG servers, use the **logging source-interface-ipv6** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

logging source-interface-ipv6 *interface-id*

no logging source-interface-ipv6

Parameters

interface-id—Specifies the source interface.

Default Configuration

The IPv6 source address is the defined IPv6 address of the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the minimal IPv6 address defined on the source interface with the scope of the destination IPv6 address is applied.

If there is no available IPv6 source address, a SYSLOG message is issued when attempting to communicate with an IPv6 SYSLOG server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# logging source-interface-ipv6 vlan 100
```

logging aggregation on

To control aggregation of SYSLOG messages, use the **logging aggregation on** Global Configuration mode command. If aggregation is enabled, logging messages are displayed every time interval (according to the aging time specified by logging aggregation aging-time, on page 1124). To disable aggregation of SYSLOG messages, use the **no** form of this command.

Syntax

logging aggregation on

no logging aggregation on

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Global Configuration mode

Example

To turn off aggregation of SYSLOG messages:

```
switchxxxxxx(config)# no logging aggregation on
```

logging aggregation aging-time

To configure the aging time of the aggregated SYSLOG messages, use the **logging aggregation aging-time** Global Configuration mode command. The SYSLOG messages are aggregated during the time interval set by the aging-time parameter. To return to the default, use the **no** form of this command.

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
```

logging origin-id

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

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”
```

logging cbd module

To define supported modules for Cisco Business Dashboard (CBD) logging, use the **logging cbd module** Global Configuration mode command. To restore the default, use the **no** form of this command.

Syntax

logging cbd module {*module* [*module2 … module6*] | ***none*** | **all}**

no logging cbd module

Parameters

- ***module*** - list includes: ***call-home, discovery, northbound, services, southbound, system***. The list replaces the previously configured list.
- **none** — disable logging for all modules.
- **all** — enable logging for all modules.

Default Configuration

Logging CBD is enabled on all modules.

Command Mode

Global Configuration mode

User Guidelines

This setting affect the CBD agent logging.

Example

The following example enables logging messages of all CBD modules.

```
switchxxxxxx(config)# logging cbd module all
```

logging cbd level

To limit messages logged of the Cisco Business Dashboard (CBD) to messages to a specific severity level, use the **logging cbd level** Global Configuration mode command. To restore the default, use the **no** form of this command.

Syntax

logging cbd level *level*

no logging cbd level

Parameters

level—Specifies the severity level of logged messages displayed on the console. The possible values are: errors, warnings, informational and debugging. This enable logging of messages with this level or higher.

Default Configuration

Informational.

Command Mode

Global Configuration mode

Example

The following example limits logging messages of the CBD to messages with severity level **errors**.

```
switchxxxxxx(config)# logging cbd errors
```

show logging

To display the logging status and SYSLOG messages stored in the internal buffer, use the **show logging** Privileged EXEC mode command.

Syntax

show logging

Parameters

This command has no arguments or keywords.

Default Configuration

None

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.
```

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
Logging cbd level: Informational
Logging cbd  modules Enabled: call-home
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
```

show logging file

To display the logging status and the SYSLOG messages stored in the logging file, use the **show logging file** Privileged EXEC mode command.

Syntax

show logging file

Parameters

This command has no arguments or keywords.

Default Configuration

None

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.
```

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
1-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#
```

show syslog-servers

To display the SYSLOG server settings, use the **show syslog-servers** Privileged EXEC mode command.

Syntax

show syslog-servers

Parameters

This command has no arguments or keywords.

Default Configuration

None

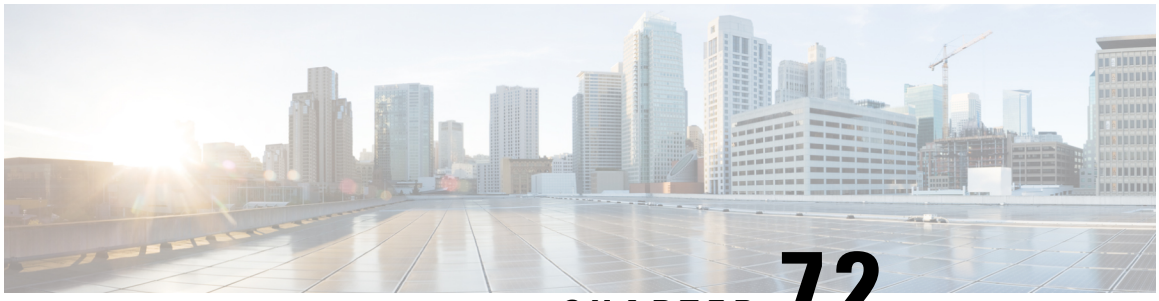
Command Mode

Privileged EXEC mode

Example

The following example provides information about the SYSLOG servers.

```
switchxxxxxx# show syslog-servers
Source IPv4 interface: vlan 1
Source IPv6 interface: vlan 10
Device Configuration
--------------------
IP address    Port   Facility Severity  Description
------------- ----   --------- -------- --------------
1.1.1.121     514    local7    info
3000::100     514    local7    info
OOB host Configuration
----------------------
IP address    Port   Facility Severity  Description
------------- ----   --------- -------- --------------
2.1.1.200     514    local7    warning
```



CHAPTER 72

Surveillance VLAN

This chapter contains the following sections:

- surveillance-vlan vlan-id, on page 1131
- surveillance-vlan enable (Interface), on page 1132
- surveillance-vlan cos, on page 1133
- surveillance-vlan aging-timeout, on page 1133
- surveillance-vlan cos, on page 1134
- Surveillance-vlan traffic-source, on page 1135
- Show surveillance-vlan, on page 1136
- show surveillance-vlan interface, on page 1136

surveillance-vlan vlan-id

To globally enable the ASV (Auto Surveillance VLAN) feature and select the surveillance VLAN ID, use the surveillance-vlan command in Global Configuration mode. Use the no form of this command to disable the feature.

Syntax

surveillance-vlan vlan-id *vlan-id*

no surveillance-vlan vlan-id

Parameters

vlan-id—The ID of the surveillance VLAN

Default Configuration

The ASV feature is disabled.

Command Mode

Global Configuration mode

User Guidelines

The VLAN assigned as the ASV must be an existing static VLAN.

When activating the ASV feature, the IGMP and MLD snooping and querier features become enabled on the VLAN and globally (if disabled). In addition, the bridge multicast filtering global setting is enabled (if disabled).

The Surveillance VLAN must be different form the following VLANs:

- Voice VLAN
- Unauthenticated VLAN
- Guest VLAN
- Private VLAN

The command can be used to modify the VLAN ID of an existing ASV VLAN. In this case the user will be prompted to confirm the configuration, as the change of the ASV VLAN ID may cause changes to VLAN membership on interfaces on which ASV is enabled (command surveillance-vlan enable (Interface)).

Example

The following example enables the ASV feature on VLAN 3:

```
switchxxxxxx(config)# surveillance-vlan vlan-id 3
```

surveillance-vlan enable (Interface)

To enable the ASV feature on an interface, use the surveillance-vlan enable Interface Configuration mode command. To disable the feature on an interface, use the no form of this command.

Syntax

surveillance-vlan enable

no surveillance-vlan enable

Default Configuration

The ASV feature is disabled on all interfaces.

Command Mode

Interface Configuration mode

User Guidelines

The ASV feature can only be enabled on interfaces whose Switchport Mode is Access or General.

Access mode should be used for interfaces who will be connected to a single surveillance device.

General mode should be used to interfaces connected to other network nodes that may be then connected to multiple surveillance devices.

If traffic from a source defined as a surveillance source is detected on an interface with the ASV feature enabled, the interface becomes a member in the surveillance VLAN.

The VLAN priority tag of the surveillance traffic forwarded on this interface will be set to the CoS value defined in the surveillance-vlan cos command.

When traffic from the surveillance source stops and the feature aging-timeout elapses, the interface is removed from the surveillance VLAN and resumes its original static VLAN membership.

In access mode, when an interface is added to the surveillance VLAN, it is removed from its original membership while it is a member of the surveillance-VLAN.

In general mode, the surveillance traffic will be routed on the surveillance VLAN while non-surveillance traffic will use the original VLAN membership of the interface.

The feature cannot be enabled on an interface if it is assigned by RADIUS to a VLAN.

Example

The following example enables the ASV feature on gi1/0/2.

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# surveillance-vlan enable
```

surveillance-vlan cos

To define the CoS value for remarking the VLAN Priority tag (CoS) of surveillance traffic detected on interfaces that are enabled, use the surveillance-vlan cos command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

surveillance-vlan cos *cos*

no surveillance-vlan *cos*

Parameters

- cos—The class of service applied to surveillance traffic. (Range: 0-7)

Default Configuration

By default the surveillance traffic is remarked with CoS 5.

Command Mode

Global Configuration mode

Example

The following example sets the CoS to 3:

```
switchxxxxxx(config)# surveillance-vlan cos 3
```

surveillance-vlan aging-timeout

To configure the aging timeout of surveillance VLAN membership, use the surveillance-vlan aging-timeout command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

surveillance-vlan aging-timeout minutes

no surveillance-vlan aging-timeout

- minutes—The amount of time after surveillance traffic stops on the interface before the interface is removed from the ASV. (Range: 1-43200)

Parameters

minutes—The amount of time in minutes after surveillance traffic stops on an interface before the interface is removed from the ASV. (Range: 1-43200)

Default Configuration

1440 minutes.

Command Mode

Global Configuration mode

Example

The following example sets the ASV aging timeout to 12 hours:

```
switchxxxxxx(config)# surveillance-vlan aging-timeout 720
```

surveillance-vlan cos

To define the CoS value for remarking the VLAN Priority tag (CoS) of surveillance traffic detected on interfaces that are enabled, use the surveillance-vlan cos command in Global Configuration mode. To restore the default configuration, use the no form of this command.

Syntax

surveillance-vlan cos *cos*

no surveillance-vlan *cos*

Parameters

- cos—The class of service applied to surveillance traffic. (Range: 0-7)

Default Configuration

By default the surveillance traffic is remarked with CoS 5.

Command Mode

Global Configuration mode

Example

The following example sets the CoS to 3:

```
switchxxxxxx(config)# surveillance-vlan cos 3
```

Surveillance-vlan traffic-source

To add a traffic source to be tracked by the ASV feature, use the surveillance-vlan traffic-source command in Global Configuration mode. Use the no form of this command to delete a traffic source from the table.

Syntax

surveillance-vlan traffic-source default | {**mac** *mac-address*|**oui** *OUI*} [**description** description]}

no surveillance-vlan traffic-source {**mac** *mac-address*|**oui** *OUI*}

Parameters

- *mac-address*—A unicast MAC address which would be added to the traffic-source table.
- *oui*—A three octet MAC address prefix which would be added to the traffic-source table.
- *description*—A description of the surveillance traffic source (length: up to 32 characters).

Default Configuration

The table is empty.

Command Mode

Global Configuration mode

User Guidelines

The traffic source table contains MAC and OUI entries. If traffic from a source matching these entries is received on an interface with the ASV feature enabled, the interface will be added to the Auto Surveillance VLAN.

Examples

The following example adds an OUI entry to the table:

```
switchxxxxxx(config)# surveillance-vlan traffic-source oui a0:bb:cc
```

The following example adds a MAC entry to the table with a description:

```
switchxxxxxx(config)# surveillance-vlan traffic-source mac 12:44:4a:4c:13:ec
description floor1_sec
```

The following example deletes a mac based entry from the table:

```
switchxxxxxx(config)# no surveillance-vlan traffic-source mac
12:44:4a:4c:13:ec
```

Show surveillance-vlan

To display the ASV global settings and status and the traffic source table, use the show surveillance-vlan command in Privileged EXEC mode.

Syntax

show surveillance-vlan

Command Mode

Privileged EXEC mode

User Guidelines

The command shows the global settings of the ASV feature and the traffic source table. The traffic source table has the following columns:

- MAC/OUI: The MAC or OUI prefix of this traffic source.
- Description: A description of the traffic source.
- Active: This value is Yes if traffic from this source was detected on any interface with the ASV feature enable that has not timed out due to the aging timeout.
- Interface: A list of interfaces with the ASV feature enabled that detected traffic from this source.

Example

This command shows the global status and configurations of the ASV feature.

The column Active in the Surveillance Traffic Sources table indicates that there is a current flow from this source which is not yet aged out of the FDB. The interfaces column shows the interfaces where traffic matching this source OUI or MAC is currently received.

The following example shows the output of the command:

```
switchxxxxxx# show surveillance-vlan
Surveillance VLAN is enabled on VLAN 5
Aging timeout: 1440 minutes
CoS: 5
Surveillance-Traffic sources
MAC/OUI Description Active Interface
================ =========== ====== =========
00:03:C5 Mobotix Yes ge1/2, LAG8
00:04:7D Pelco No
10:22:33:12:44:22 RND-Server Yes ge1/4
```

show surveillance-vlan interface

This command shows the interface status and configuration related to the ASV feature.

To display the ASV interface settings and status, use the show surveillance-vlan interface command in Privileged EXEC mode.

Syntax

show surveillance-vlan interface

Command Mode

Privileged EXEC mode.

User Guidelines

The command shows the interface settings of the ASV feature on the interfaces of the device.

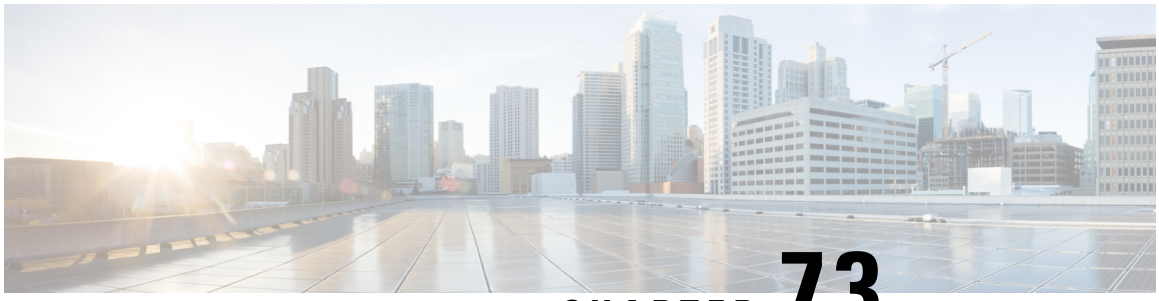
The settings table has the following columns:

- Interface: The interface whose status the row shows.
- Enabled: A boolean indication on whether the ASV feature is enabled on the interface.
- Active: This value is Yes if the interface became a member of the ASV VLAN (even if the MAC address forwarding table does not include an entry for the surveillance traffic source address).

Example

The following example shows the output of the command:

```
Switchxxxxxx# show surveillance-vlan interface
Interface Enabled Active
========= ======= ======
ge1/1     Yes     No
ge1/2     Yes     Yes
ge1/3     No      No
```



CHAPTER 73

System Management Commands

This chapter contains the following sections:

- disable ports leds, on page 1140
- dying-gasp enable, on page 1140
- hostname, on page 1141
- interface beacon-light, on page 1142
- monitor capture, on page 1143
- monitor capture buffer, on page 1144
- monitor capture clear, on page 1145
- monitor capture control-plane, on page 1146
- monitor capture crash-export, on page 1148
- monitor capture export, on page 1148
- monitor capture match, on page 1150
- monitor capture start, on page 1151
- monitor capture stop, on page 1152
- reload, on page 1153
- reload factory-default, on page 1154
- resume, on page 1155
- service cpu-utilization, on page 1156
- show cpld version, on page 1156
- show cpu input rate, on page 1157
- show cpu utilization, on page 1157
- show dying-gasp packets, on page 1158
- show dying-gasp status, on page 1159
- show environment, on page 1159
- show inventory, on page 1161
- show monitor capture, on page 1162
- show platform certificate, on page 1164
- show platform hardware integrity, on page 1169
- show platform integrity, on page 1170
- show reload, on page 1172
- show sessions, on page 1173
- show software versions, on page 1174
- show system, on page 1175

- show system languages, on page 1176
- show system tcam utilization, on page 1177
- show services tcp-udp, on page 1177
- show tech-support, on page 1178
- show system fans, on page 1179
- show system sensors, on page 1181
- show system id, on page 1182
- show ports leds configuration, on page 1183
- show users, on page 1183
- show hardware version, on page 1184
- show hardware components, on page 1184
- system light, on page 1186
- system recovery, on page 1186
- system reset-button disable, on page 1187

disable ports leds

To turn **off** the LEDs on all ports on a device, use the **disable ports leds** Global Configuration mode command.

To set the LEDs of all the ports on the device to their current operational status of the port, use the **no disable ports leds** command.

Syntax

disable **ports leds**

no disable **ports leds**

Parameters

This command has no arguments or keywords.

Default Configuration

The default is **no disable port leds**; that is the LEDs of all the ports reflect their current status.

Command Mode

Global Configuration mode

Examples

The following example turns off the port LEDs.

```
switchxxxxxx(config)# disable ports leds
```

dying-gasp enable

This command enables the dying gasp feature and selects the methods it uses to send the message and their priority. Using the no form of the command returns to the default configuration (disables the feature).

Syntax

dying-gasp enable *method1 [method2…]*

no dying-gasp enable

Parameters

Method1 [method2…]: A list of the methods used to send dying gasp messages. The order of the methods indicates the priority between the methods. At least one method must be entered to enable the feature. A method not included in the list will not be used to send dying gasp messages.

The possible methods are: snmp-traps, syslog

Default Configuration

By default, dying gasp is disabled.

Command Mode

Global Configuration mode.

hostname

To specify or modify the device host name, use the **hostname** Global Configuration mode command. To remove the existing host name, use the **no** form of the command.

Syntax

hostname *name*

no hostname

Parameters

Name—Specifies the device host name. (Length: 1-58 characters). 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)#
```

interface beacon-light

To activate the LED of the specified interface(s), use the interface beacon-light Privileged EXEC mode command. Use the interface beacon-light stop command to stop interface beacon-light operation.

Syntax

interface beacon-light [**duration** *seconds*] {*interface-id* | *interface-id-list*}

interface beacon-light stop

Parameters

- duration *seconds* – (optional) The duration in seconds for port LED activation. If unspecified, the LED activity duration is 60 seconds. (Range: 5–3600 seconds)
- *interface-id* – Specified the interface to locate. The specified interface can be one ofthe following types: Ethernet port, or port-channel
- *interface-id-list* – Specifies multiple interfaces. The list can include one or more of the following interface types: Ethernet port or port-channel.
- **stop**—Terminates. on all ports, the LED activity triggered previously by the command.

Default configuration

If the command does not include the duration parameter, then the LED activity duration will be set to 60 seconds.

Command Mode

Privileged EXEC mode

User Guidelines

This command is used to indicate the location of the interface(s) specified in the command by activating the port LED of the specified interfaces. If a port-channel is specified in the command then all the interfaces that are member in the port channel (active and not active) will provide LED indication.

Each activation of the command terminates the LED indication(s) generated by the previous command (if it is still active), and the new LED action is applied according to the parameters of the new command (interfaces and duration).

The **interface beacon-light stop** command stops on all of the interfaces the LED activity related to port, and resumes regular port LED activity.

Examples

Example 1: The following example activates the LED on interface gi1 for the default duration of 60:

02-Apr-2023 12:30:14 %Environment-I-PORT-BEACON-CHNG: Interface beacon operation activated for 60 seconds

Example 2: The following example activates the LED on a list of interfaces for the duration of 10 minutes (600 seconds):

switchxxxxxx# interface beacon-light duration 600 gi1,gi9, po2

02-Apr-2023 12:30:02 %Environment-I-PORT-BEACON-CHNG: Interface beacon operation activated for 600 seconds

Example 3: The following example terminates LED activity related to port locate (if active) on all the device interfaces:

switchxxxxxx# interface beacon-light stop

02-Apr-2023 12:54:22 %Environment-I-PORT-BEACON-CHNG: Interface beacon operation terminated – user intervention

monitor capture

To create an On-board Packet Capture (OPC) session, use the monitor capture Privileged EXEC mode command. Use the no form of the command to deleted an OPC session.

Syntax

monitor capture *capture-name*

no monitor capture *capture-name*

Parameters

- *capture-name* - Specifies the name of the OPC session (Range: 1-32 characters)

Default configuration

OPC sessions do not exist by default.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to create an OPC session. Up to 4 OPC sessions are supported.

An OPC session will also be created by configuring one of the OPC settings on a new OPC session.

The monitor capture control-plane and monitor capture match settings are mandatory in order to activate/start the capture session (command monitor capture start). The other OPC session settings are optional.

Use the no monitor capture capture-name command to delete the OPC session and all its settings.

Examples

Example 1: In the following example OPC session cap1 is created:

switchxxxxxx# **monitor capture** cap1

Example 2: In the following example the user attempts to create OPC session cap1 which already exists:

switchxxxxxx# monitor capture cap1

Entry already exists

Example 3: In the following example the creation of cap5 OPC session fails since 4 other capture sessions have already been defined:

switchxxxxxx# monitor capture cap5

Unable to create capture - maximum supported capture point count reached

Example 4: The following example deletes OPC session cap1:

switchxxxxxx# no monitor capture cap1

monitor capture buffer

To configure the buffer settings for an On-board Packet Capture (OPC) session, use the **monitor capture buffer** Privileged EXEC mode command. Use the no form of the command to restore the buffer settings to the default values.

Syntax

monitor capture *capture-name* **buffer {circular [size** buffer-size] | **size** buffer-size **[circular]**}

monitor capture capture-name **buffer [size] [circular]**

Parameters

- *capture-name* - Specifies the name of the OPC session (Range: 1-32 characters)
- **circular [size** buffer-size] - Sets the buffer mode to circular and optionally also defines the buffer size. If the size parameter is not specified the default buffer size will be used. (buffer size range: 1- 20 MB)
- **size** *buffer-size* [circular] - Sets the buffer size and optionally also sets the buffer mode to circular. If the **circular** parameter is not specified the linear buffer mode will be used. (**buffer size** range: 1- 20 MB (megabyte))

Default configuration

The default buffer mode is linear.

The default buffer size is 5 MB.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to define the buffer mode and/or the buffer size for an OPC session. If the circular parameter is not defined then the default buffer mode will be used (linear mode).

When capturing packets in linear buffer mode - once the buffer is full, the capture session is terminated. When the buffer is full in this mode, the capture session cannot be restarted.

When capturing packets in circular buffer mode - packet capture continues even if the buffer is full. Existing packet data will be overwritten by the new packets (FIFO)

If the size parameter is not defined then the default buffer size will be used (5 MB).

This command can be applied only for an OPC session that is not active.

If the OPC session named by the user already exists then this command will apply the buffer settings to the existing OPC session. If the OPC session named by the user does not exist, then this command will create the OPC session with the specified buffer settings. Up to 4 OPC sessions are supported.

Use the no monitor capture capture-name buffer form of the command to return both buffer mode and size to the default settings.

Use the no monitor capture capture-name buffer size circular form of the command to return both buffer mode and size to the default settings.

Use the no monitor capture capture-name buffer circular form of the command to return the OPC session buffer mode to the default setting (linear mode).

Use the no monitor capture capture-name buffer size form of the command to return the OPC session buffer size to the default settings (5 MB).

Examples

Example 1: The following command sets the buffer mode of OPC session cap2 to circular. If cap2 does not exist, this command will also create the OPC session:

switchxxxxxx# monitor capture cap2 buffer circular

Example 2: The following example defines the maximum buffer size (20 MB) for OPC session cap2. If cap2 does not exist, this command will also create the OPC session:

switchxxxxxx# monitor capture cap2 buffer size 20

Example 3: In the following example buffer size allocation failed because the size allocated to all buffers exceeds the total memory allocated for all OPC buffers (20 MB):

switchxxxxxx# monitor capture cap2 buffer size 10

Unable to allocate buffer - maximum supported buffer size reached

Example 4: The following example sets the cap2 OPC session buffer size to the default size:

switchxxxxxx# no monitor capture cap2 buffer size

monitor capture clear

To clear the On-board Packet Capture (OPC) session buffer, use the monitor capture clear

Privileged EXEC mode command.

Syntax

monitor capture *capture-name* clear

Parameters

- *capture-name* - The name of the OPC session (Range: 1-32 characters)

Default configuration

None

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to clear the buffer of an an OPC session. This OPC session buffer can be cleared for both active and in-active OPC sessions. A confirmation message will require the user to confirm the buffer clear operation.

Examples

Example 1: The following command clears the buffer of OPC session cap1:

switchxxxxxx# monitor capture cap1 clear

Captured data will be deleted [clear]? (Y/N)[Y] Y

monitor capture control-plane

To configure the control plane as a source for an On-board Packet Capture (OPC) session, and to define the direction of the capture, use the monitor capture control-plane Privileged EXEC mode command. Use the no form of the command to remove the control plane or a capture direction from the capture session.

Syntax

monitor capture *capture-name* **control-plane {in | out | both}**

no monitor capture *capture-name* **control-plane [in | out | both]**

Parameters

- *capture-name* - The name of the OPC session (Range: 1-32 characters)
- **control-plane** - Specifies the control plane as a source for the OPC session.
- **{in | out | both}** - Defines the direction of the traffic to capture

Default configuration

The control plane is not defined as a source for an OPC session.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to define that the control plane is a source for an OPC session, and to define the direction of traffic to capture. The control plane is the control traffic to and from the system CPU. This command is mandatory for an OPC session. If the control plane is not defined as a source for an OPC session then the activation of the session (command monitor capture start) will fail.

Use the in, out, or both keyword to define the direction of the traffic that will be captured. The in direction means that only the traffic to the CPU will be captured. The out direction means that only the traffic from the CPU will be captured. The both direction means that both traffic from and to the CPU will be captured.

If the command is defined multiple times, the direction defined in the most recent command will be the used as the capture direction.

This command can be applied only for an OPC session that is not active.

If the OPC session named by the user already exists then this command will enable control plane packet capture for the existing OPC session. If the OPC session named by the user does not exist, then this command will create the OPC session and enable control plane packet capture for it. Up to 4 OPC sessions are supported.

Use the no monitor capture capture-name control-plane command to disable control-plane capturing.

Use the no monitor capture capture-name control-plane both command to disable control-plane capturing.

Use the no monitor capture capture-name control-plane in command to disable ingress traffic control-plane capturing. If only the in direction was defined for this OPC session, then monitor capture for the control plane will be disabled. If the out or both direction were defined for this capture session, then the capture will continue on the output traffic direction of the control plane.

Use the no monitor capture capture-name control-plane out command to disable egress traffic control-plane capturing. If only the out direction was defined for this OPC session, then monitor capture for the control plane will be disabled. If the in or both direction were defined for this capture session, then the capture will continue on the ingress traffic direction of the control plane.

Examples

Example 1: The following command enables packet capture on both directions of the control plane for OPC session cap3. If cap3 does not exist, this command will also create the OPC session:

switchxxxxxx# monitor capture cap3 control-plane both

Example 2: The following example enables traffic capture on the ingress control plane traffic for an existing OPC session cap3. If cap3 does not exist, this command will also create the OPC session:

switchxxxxxx# monitor capture cap3 control-plane in

Example 3: The execution of the command in the next example fails because the capture has been activated on OPC session cap3:

switchxxxxxx# monitor capture cap3 control-plane out

Cannot modify - Capture point is currently active.

Example 4: The following example disables control plane traffic capture for cap3 OPC session:

switchxxxxxx# no monitor capture cap3 control-plane

Example 5: The following example disables traffic capture only for the control plane egress direction:

switchxxxxxx# no monitor capture cap3 control-plane out

monitor capture crash-export

To define the USB storage device the as the destination for the packet capture file related to a system crash use the monitor capture crash-export Privileged EXEC mode command. Use the no form of the command to return the destination storage location to the local flash device.

Syntax

monitor capture crash-exort usb

no monitor capture crash-exort

Parameters

N/A

Default configuration

A packet capture file related to a system crash is saved to the local flash.

Command Mode

Privileged EXEC mode

User Guidelines

If an active OPC session is capturing packets during the time that a software related system crash occurs, then the contents of the capture buffer will be automatically saved to a file in the main directory of the local flash. The file name format is "crash_dd-MMM-YYYY hhmm.pcap". The ToD is provided by the system clock.

Use the monitor capture crash-exort usb command to define the USB storage device, as the destination storage device instead of the flash.

To return the destination location to the local flash use the no monitor capture crash-exort command.

Examples

Example 1: The following command defines the USB as the destination storage device for a capture file that was active during a software related device crash:

switchxxxxxx# monitor capture crash-export usb

Example 2: The following command returns the local flash as the destination storage device:

switchxxxxxx# no monitor capture crash-export

monitor capture export

To export the packets in an On-board Packet Capture (OPC) buffer to a file use the monitor capture export Privileged EXEC mode command.

Syntax

monitor capture capture-name exort dst-url

Parameters

- *capture-name* - The name of the OPC session (Range: 1-32 characters)
- *dst-url*—The URL of the destination file. Only the local flash path or the USB path can be specified.

Default configuration

None

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to export packets from an OCP buffer to a pcap capture file. An OPC buffer memory can be exported only while if the capture session is the in-active state. The Export operation does not clear the capture buffer.

The destination-url can be specify a path on the local flash or a path on the USB storage device. If a filename is specified without a path then the packets will be copied to a file in the current flash directory.

If the file name specified in the command does not exist then it will be created automatically at the specified path. If the file name specified in the command already exists, then the user will be prompted to confirm the overwrite of the existing file.

Examples

Example 1: The following command exports the packets of the cap1 OPC session buffer to a new file on the local flash:

switchxxxxxx# monitor capture cap1 export flash:/cap1.pcap

29-May-2024 18:57:04 %COPY-I-FILECPY: Files Copy - source URL capture://cap1 destination URL flash://cap1.pcap

29-May-2024 18:57:05 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 1048529 bytes copied in 00:00:01 [hh:mm:ss]

Example 2: The following command exports the packets of the cap1 OPC session buffer to an existing file on the local flash:

switchxxxxxx# monitor capture cap1 export flash:/cap1.pcap

Overwrite file [flash://cap1.pcap].... (Y/N)[N] ?Y

29-May-2024 18:58:56 %COPY-I-FILECPY: Files Copy - source URL capture://cap1 destination URL flash://cap1.pcap

29-May-2024 18:58:57 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 1048529 bytes copied in 00:00:01 [hh:mm:ss]

Example 3: The execution of the export operation in the next example fails because the capture buffer of cap2 OPC session does not contain any packets:

switchxxxxxx# monitor capture cap2 export flash:/cap2.pcap

29-May-2024 19:02:35 %COPY-I-FILECPY: Files Copy - source URL capture://cap2

destination URL flash://cap2.pcap

29-May-2024 19:02:35 %COPY-W-TRAP: The copy operation has failed

Copy: Unable to export capture - cap2 buffer has no packets

monitor capture match

To define a capture filter for an On-board Packet Capture (OPC) session, use the monitor capture match Privileged EXEC mode command. Use the no form of the command to remove the capture filter.

Syntax

monitor capture *capture-name* **match any**

no monitor capture *capture-name* **match**

Parameters

- *capture-name* - The name of the OPC session (Range: 1-32 characters)
- **any** - Specifies that all packets types will be captured

Default configuration

Monitor capture traffic filter is not configured.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to define a filter for the packets that the specified OPC session will capture.

Only packets matching the filter will be captured. The only filter that is supported is any which will capture packet types.

This command is mandatory for an OPC session. If the capture filter is not defined then the activation of the session (command monitor capture start) will fail.

This command can be applied only for an OPC session that is not active.

If the OPC session named by the user already exists then this command will define the capture filter for the existing OPC session. If the OPC session named by the user does not exist, then this command will create the OPC session and apply to it the specified capture filter. Up to 4 OPC sessions are supported.

Use the **no monitor capture** capture-name **match** command to remove the filter from the capture session. If the filter is removed the OPC session cannot be activated (command monitor capture start).

Examples

Example 1: The following command applies the any traffic filter to OPC **session cap4**. If cap4 does not exist, this command will also create the OPC session:

switchxxxxxx# **monitor capture** cap4 match any

Example 2: The following example removes the any packet filter from OPC session **cap4**:

switchxxxxxx# **no monitor capture** cap4 **match**

monitor capture start

To start the capture operation for an On-board Packet Capture (OPC) session, use the monitor capture start Privileged EXEC mode command.

Syntax

monitor capture capture-name start

Parameters

- *capture-name* - The name of the OPC session (Range: 1-32 characters)

Default configuration

The OPC session is not active.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to activate/ start the packet capture for the specified OPC session. It is recommended to check CPU utilization before activating a OPC session. Only one session can be activate. This means that an attempt to activate more than one OPC session will fail.

An OPC session can be activated only if it is defined with a capture filter (command monitor capture match) and capture source (command monitor capture control-plane).

An OPC session that was stopped (command monitor capture stop) can be re-started after it was stopped, unless the buffer is full and the buffer mode is set to linear. In case a capture is restarted then the packets captured in the new capture session will be appended to the existing packets stored in the buffer. If the capture buffer is cleared (command monitor capture clear) then the capture can be re-started even if the buffer was previously full and the buffer mode was linear.

Examples

Example 1: In the following example the command successfuly starts the packet capture for

OPC session cap1:

switchxxxxxx# monitor capture cap1 start

29-May-2024 11:14:37 %BUFCAP-I-ENABLE: Capture Point cap1 enabled

Started capture point : cap1

Example 2: In the following example the command to start the packet capture for OPC session cap2 fails because cap1 session is still active:

switchxxxxxx# no monitor capture cap2 start

Capture cap1 is already active - cannot start the capture.

Example 3: In the following example the command to start the packet capture for OPC

session **cap3** fails because a source interface (the control plane) was not defined:

switchxxxxxx# no monitor capture cap3 start

Unable to activate capture - A source interface is not defined on the capture point

Example 4: In the following example the command to start the packet capture for OPC

session cap4 fails because the buffer for this OPC session is full (buffer mode is linear):

switchxxxxxx# no monitor capture cap4 start

Unable to activate capture - capture buffer is full (linear mode)

monitor capture stop

To stop the capture operation of an On-board Packet Capture (OPC) session, use the monitor capture stop Privileged EXEC mode command.

Syntax

monitor capture *capture-name* stop

Parameters

- *capture-name* - The name of the OPC session (Range: 1-32 characters)

Default configuration

Not applicable.

Command Mode

Privileged EXEC mode

User Guidelines

Use this command to stop the capture of packets that was started using the monitor capture start command.

An OPC session can be re-started (command monitor capture start) after it was stopped, unless the buffer is full and the buffer mode is set to linear. In case a capture is restarted then the packets captured in the new capture session will be appended to the existing packets stored in the buffer. If the capture buffer is cleared (command monitor capture clear) then the capture can be re-started even if the buffer was previously full and buffer mode was linear.

Examples

Example 1: In the following example packet capture is stopped for OPC session cap1:

switchxxxxxx# monitor capture cap1 stop

Stopped capture point : cap1

Example 2: In the following example the command to stop the packet capture for OPC session cap2 fails because cap2 session is not active:

switchxxxxxx# no monitor capture cap2 stop

Capture cap2 is not active

Example 3: In the following example the command to stop the packet capture for OPC session cap6 fails because cap6 does not exit (was not created):

switchxxxxxx# no monitor capture cap6 stop

No such instance exists.

reload

To reload the operating system at a user-specified time, use the **reload** Privileged EXEC mode command.

Syntax

reload [**in** [hhh:mm | mmm] | **at** hh:mm [day month]] | **cancel**]

Parameters

- **in** hhh:mm | mmm—(Optional) 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—(Optional) 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**—(Optional) Number of the day in the range from 1 to 31.
- **month**—(Optional) Month of the year.
- **cancel**—(Optional) Cancels a scheduled reload.

Default Usage

None

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.

Example 1: The following example reloads the operating system on all units of a stack system or on the single unit of a standalone system.

```
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 on all units of a stack system or on the single unit of a standalone system.

```
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 of a stack system or on the single unit of a standalone system.

```
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.
```

reload factory-default

Use the reload factory-default Privileged EXEC mode command to reload the stack or a specific unit in a stack and return the settings to factory default.

Syntax

reload factory-default [unit unit-id]

Parameters

- [**unit** unit-id]—(Optional) reset to factory default and reload only the specified unit. Other units in the stack will not reset or reload. If this parameter is not specified, then all the units in the stack will reset to factory default and reload.

Default Usage

By default, all the units in the stack are reset to factory default settings and then reload.

Command Mode

Privileged EXEC mode

User Guidelines

This command will reset to factory default settings all of the units in the stack. If the [unit unit-id] parameter is specified only the specified unit will be reset to factory defaults. The command has the same effect as pressing the device reset button to initiate a factory default reset and device reload. The stack settings, configuration files, syslog files and other configuration related files will be erased. Units that are reset to factory default will disconnect from the stack and stack topology will change. This may create a disconnection between units in the stack.

If the command specifies the Active Unit in the [unit unit-id] parameter, then the stack will continue to operate only if one of the remaining units is a Standby Unit.

Examples

Example 1: The following example resets to factory default and reloads all of the units in the stack.

```
switchxxxxxx> reload factory-default
This command will reset to factory default and reload all of the units in the
stack. It is highly recommended to backup the stack configuration before
applying this command.
```

Example 2: The following example resets to factory default and reloads only unit number 3.

```
switchxxxxxx> reload factory-default unit 3
This command will reset to factory default and reload the selected unit. The
unit will disconnect from the stack and will no longer be a member of the
stack. The disconnection of the unit will affect the stack topology and may
disconnect other units in the stack.
Do you want to continue? (y/n) [Y]
```

resume

To enable switching to another open Telnet session, use the **resume** EXEC mode command.

Syntax

resume [*connection*]

Parameters

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

Default Configuration

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

Command Mode

Privileged EXEC mode

Example

The following command switches to open Telnet session number 1.

```
switchxxxxxx> resume 1
```

service cpu-utilization

To enable measuring CPU utilization, use the **service cpu-utilization** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

service cpu-utilization

no service cpu-utilization

Parameters

This command has no arguments or keywords.

Default Configuration

Measuring CPU utilization is enabled.

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
```

show cpld version

To display the device CPLD code version, use the **show cpld version** User EXEC mode command.

Syntax

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

Parameters

unit [*unit-id*]—Specifies the unit number (Range: 1 – 4). If not specified, the command will display CPLD code version for all units in stack.

Command Mode

User EXEC mode

Example 1 - The following example displays the CPLD version of all units in stack.

```
switchxxxxxx> show cpld version
Unit ID     Unit Type    CPLD code Version
----       -----------     -------------
1          CBS350-48P-4X      1.0.1
2                  CBS350-48P-4X      1.0.2
```

Example 2 - The following example displays the CPLD version where a unit in stack does not have a CPLD.

```
switchxxxxxx> show cpld version
Unit ID     Unit Type    CPLD code Version
----       -----------     -------------
1          CBS350-48P-4X      Not Supported
2                  CBS350-48P-4X      1.0.2
```

show cpu input rate

To display the rate of input frames to the CPU in packets per seconds (pps), use the **show cpu input rate** User EXEC mode command.

Syntax

show cpu input rate

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

Example

The following example displays CPU input rate information.

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

show cpu utilization

To display information about CPU utilization, use the **show cpu utilization** Privileged EXEC mode command.

Syntax

show cpu utilization

Parameters

This command has no arguments or keywords.

Default Usage

None

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%
```

show dying-gasp packets

To display information on the packets that will be sent out in case of a dying-gasp event, use the show dying-gasp packets command in Privileged EXEC mode.

Syntax

show dying-gasp packets

Command Mode

Privileged EXEC mode

User Guidelines

The command shows information on the packets that will be sent out if the switch loses power and sends out dying gasp packets.

Information will be provided for each SYSLOG server and SNMP trap receiver that will be sent dying gasp messages. This information includes:

The recipient IP address

The outbound interface

The local IP address

The local MAC address

The next hop IP and MAC addresses.

It is possible to use the syslog or snmp-trap keywords in the command in order to only see the packets of a single method.

Examples

Example: The following example shows the output of the command:

```
switchxxxxxx# show dying-gasp packets
Syslog packet for server 8.1.154.22, link type IP
Via interface gigabitEthernet1/0/6, local IP address 8.1.154.98
Encap type is ARPA, local MAC address 00:50:43:8a:ce:19
Next hop IP address 8.1.154.192, next hop MAC address a2:43:41:44:8a:f2
SNMP trap packet for server 6.193.2.29, link type IP
Via interface gigabitEthernet1/0/3, local IP address 6.193.2.5
Encap type is ARPA, local MAC address 00:50:43:8a:ce:19
Next hop IP address 6.193.2.45, next hop MAC address 82:a3:9c:15:cb:3d
```

show dying-gasp status

This command shows the global configuration of the Dying Gasp feature.

Examples

This example shows how to configure the show-dying-gasp-status

```
Switch000000#show dying-gasp status
Dying Gasp Status: Enabled
Method 1: Syslog
Method 2: SNMP Traps
```

show environment

To display environment information, use the **show environment** User EXEC mode command.

Syntax

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

Parameters

- **all—Displays the fan and temperature general status. If this parameter is used - a fault situation will be reported if it exists on any one of the stack units**
- **fan**—Displays the fan(s) status
- **temperature {status}—**Displays the temperature status
- **stack *[switch-number]***—(Optional) Displays detailed environment status of a stack, per each stack unit. If the switch-number is specified, the environment status of the selected device number is displayed. (Range: 1 – 4)

Command Mode

User 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** - One or more of the fans failed.
- **Fan read fail** - Reading information from one or more fans failed.
- **NA** - No fan is installed.

Temperature can be one of:

- **OK** - The temperature is below the warning threshold.
- **Warning**- The temperature is between the warning threshold and the critical threshold.
- **Critical** - the temperature is above the critical threshold.

Sensor status can be one of:

- **OK** - All Sensors on device are functioning properly.
- **Failure** - One or more of the sensors failed.
- **NA** - No sensor installed.

Example 1 - The following example displays the general environment status of a device or a stack.

```
switchxxxxxx> show environment all
```

Internal power supply Active.

```
fans OK
Sensor is OK
Temperature is OK
#EDITOR: The temperature status is OK if ALL the temperature sensors status in all the stack
 members is OK, and if the temperature of all the stack members is below the lowest threshold
 (this is calculated per stack member, if one or more of the stack members temperature is
above its specific threshold, the temperature status is FAILURE)
#EDITOR: Likewise the fan status will be OK - only if status of fans on ALL stack members
is OK (meaning no fan fail - or with redundant fan support - only 1 fan fail and redundant
 fan active
```

Example 2 - The following example displays the power status of a device or a stack.

```
switchxxxxxx> show environment power
```

Internal power supply Active.

Example 3 - The following example displays the general fan status of a device or a stack.

```
switchxxxxxx> show environment fan
fans OK
#EDITOR: The fan status is OK if the fan sensors status in ALL the stack members is OK
```

Example 4 - The following example displays the temperature status of a device or a stack.

```
switchxxxxxx> show environment temperature status
TEMPERATURE level is Warning
```

Example 5 - The following example displays the detailed environment status of a stack.

```
switchxxxxxx> show environment stack
Unit           fan Status
---            ---------
1              OK
2              Failure
3              Read fan fail
4              NA
#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
               Status       Level
---            ---------   --------------
1              OK            warning
2              Failure       NA
3              NA            NA
4              OK            OK
```

show inventory

To display product inventory list, use the **show inventory** User EXEC mode command.

Syntax

show inventory [*entity*]

Parameters

entity—Specifies the entity to be displayed. It can be a number (1 - 4) for a specific unit number in a stack, or an interface (Ethernet) name.

Command Mode

User EXEC mode

User Guidelines

Use the **show inventory** command to retrieve and display inventory information about the device, unit in stack, and connected entities such as SFPs.

In case no entity is specified the command will display information for all units in stack and all connected entities.

If the specified entity is an interface (Ethernet) name, and an SFP is not inserted into the port - Only the NAME & DESCR fields will be displayed, and DESCR will be “No SFP Inserted”.

Examples

Example 1 - The following example displays all the entities in a standalone system.

```
switchxxxxxx>  show inventory
NAME: "1", DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9, VID: V01, SN: 123456789
```

Example 2 - The following example displays a specific entity in a standalone system.

```
switchxxxxxx> show inventory gigabitethernet1/0/49
NAME: "GigabitEthernet1/0/49", DESCR: "1000M base-LX Mini-GBIC SFP Transceiver"
PID: MGBLX1,VID: V01, SN: AGC1525UR7G
```

Example 3 - The following example displays information for specific entity - where VID information cannot be read from SFP.

```
switchxxxxxx> show inventory gi1/0/1
NAME: "gi1/0/1", DESCR: "SFP-1000Base-LX"
PID: SFP-1000-LX ,VID: Information Unavailable , SN: 613bbgr8
```

Example 4 - The following example displays information for specific interface - where SFP is not inserted into the interface.

```
switchxxxxxx> show inventory gi1/0/2
NAME: "gi1/0/2", DESCR: "SFP not inserted"
```

Example 5 - The following example displays all the entities in a stacking system with two units.

```
switchxxxxxx> show inventory
NAME: "2", DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9 , VID: V01, SN: 123456789
NAME: "GigabitEthernet2/0/49", DESCR: "1000M base-LX Mini-GBIC SFP Transceiver"
PID: MGBLX1,  VID: V01, SN: AGC1525UR7G
NAME: "4", DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9 , VID: V01, SN: 123456789
```

Example 6- The following example displays information for unit 1 of the stack.

```
switchxxxxxx> show inventory 1
NAME: "1"  DESCR: "48-Port Gigabit with 4-Port 10-Gigabit Managed Switch"
PID: xx350-4x-K9  VID:  V02  SN: 402
```

show monitor capture

To display On-board Packet Capture (OPC) session information, use the show monitor capture command in Privileged EXEC mode.

Syntax

show monitor capture [*capture-name* [**parameter | buffer]**]

Parameters

- *capture-name* (optional)- Specifies the name of the OPC session (Range: 1-32 characters). If not specified the command output will display information for all OPC sessions
- **parameter** (optional) - displays the configuration lines applied to the specified OPC session
- **buffer** (optional) - displays the buffer information for the specified OPC session

Default configuration

Information for all OPC sessions is displayed.

Command mode

Privileged EXEC mode

User Guidelines

The show monitor capture command form will display configuration and status information for all OPC sessions.

The show monitor capture apture-name command form will display configuration and status information for the specified OPC session.

The show monitor capture apture-name parameter command form will display the non default configuration lines applied to the specified OPC session. This option is usefull since OPC sessions and settings are not saved to the device running configuration

The show monitor capture apture-name buffer command form will display buffer information for the specified OPC session. The ouput includes the following fields:

- buffer size - the memory allocated to this buffer in kilobytes.
- buffer used - the actual memory space this buffer consumes (in steps of 256 kilobytes)
- packets in buf - the number of packets stored in the buffer
- packets dropped - the number of packets dropped and not captured
- packet rate per second - the rate in which packets are captured to the buffer

Examples

Example 1: In the following example configuration and status information for all of the OPC sessions is displayed:

```
switchxxxxxx# show monitor capture
Status Information for Capture cap1
Target Type:
Interface: Control Plane, Direction: BOTH
Status : Active
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer size (in MB): 1
Status Information for Capture cap2
Target Type:
Interface: Control Plane, Direction: OUT
Status : Inactive
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: CIRCULAR
Buffer size (in MB): 5 (default)
Status Information for Capture cap3
Target Type:
Interface: None, Direction: NONE
Status : Inactive
Filter Details:
None
Buffer Details:
Buffer Type: LINEAR (default)
```

```
Buffer size (in MB): 5 (default)
Status Information for Capture 4
Target Type:
Interface: None, Direction: NONE
Status : Inactive
Filter Details:
None
Buffer Details:
Buffer Type: LINEAR (default)
Buffer size (in MB): 6
```

Example 2: In the following example the configuration and status information for OPC session cap1 is displayed:

```
switchxxxxxx# show monitor capture cap1
Status Information for Capture cap1
Target Type:
Interface: Control Plane, Direction: BOTH
Status : Active
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer size (in MB): 1Entry already exists
```

Example 3: In the following example the configuration lines applied to OPC session cap1 is displayed:

```
switchxxxxxx# show monitor capture cap1 parameter
monitor capture cap1 control-plane BOTH
monitor capture cap1 match any
monitor capture cap1 buffer size 1
```

Example 4: In the following example OPC session cap1 buffer information is displayed:

```
switchxxxxxx# show monitor capture cap1 buffer
buffer size (KB) : 1024
buffer used (KB) : 512
packets in buf : 4903
packets dropped : 0
Packet rate per second : 19
```

show platform certificate

Use the show platform certificate Privileged EXEC mode command to display the Active unit SUDI certificate or AIK certificate and optionally a signature over the certificates.

Syntax

show platform {sudi | attestation} certificate [sign [nonce <nonce value>]]

Parameters

- {**sudi | attestation**} - display either SUDI or Attestation (AIK - Attestation Identity Key) certificate.
- **sign**—(Optional) display a signature over the certificate
- [**nonce** <nonce value>]—(Optional) provide a nonce to use with the signature to protect from replay attacks. (range 0-4,294,967,295)

Default Usage

The certificate is displayed without a signature. If the sign parameter is specified without a nonce value then the signature will be generated without using a nonce.

Command Mode

Privileged EXEC mode

User Guidelines

The show platform certificate command displays the device SUDI or AIK (Attestation Identity Key) certificate.

The command output includes the certificate chain in PEM format, where the first certificate that is displayed is the Cisco Root CA, and the second certificate that is displayed is the Cisco published on https://www.cisco.com/security/pki/. The third certificate is the SUDI or AIK leaf certificate.

If the optional sign parameter is used, then the command output will display a signature over the certificates using either the SUDI (if sudi keyword is used) or AIK (if attestation keyword is used) private key.

The command also supports an optional [nonce <nonce value>] parameter used as part of the signature inputs to prevent replay attacks. If the [nonce <nonce value>] parameter is not provided the signed data will not include the nonce.

The command output includes a signature version. Signature value of 1 indicates that the SUDI private key was used for signing, while a signature value of 2 indicates that the AIK private key was used for signing.

Examples

Example 1: The following example displays the SUDI certificate chain without a signature:

```
switchxxxxxx> show platform sudi certificate
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a11Eb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30SecmrxkmQBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAyODA4WhgPMjA5OTA4MDkyMDU4MjdaMDExHzAdBgNVBAMTFkhpZ2ggQXNzdXJh
bmNlIFNVREkgQ0ExDjAMBgNVBAoTBUNpc2NvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAvdzeSWdDI6lRZDYRvA6JqaRvQyy6Dx1WaqI82UeKR4ZRn0ef
xMGvp4c88/VMS8WSjQO1qolMfMxqHkcSiFBOULx6Trquw4TrEf9sIuzvgJvDaEa8
IllXPwtPtNqZEIWi8jlinz2uGam93KuGPcioHfruzbDKWHL/HWFGYMgz+OKwhD3J
4NRySknQvUovfV8eWLeVOqW8rbnG3TZxv5VexOiK4jL3ObvsQPuAWUwUoo7nuFlE
GTG/VCeyCe/H8+afIScbZOkI9xejtckflnBYFVCyFxzm2H3YZatb6ohbyRXLtOPj
```

```
T3SJ+OOoYMlSLd28z727LpRbFFLGYhyWxEXDuQIDAQABo4IBgjCCAX4wDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfwYIKwYBBQUHAQEEczBxMEEG
CCsGAQUFBzAChjVodHRwczovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2Nl
cnRzL2NyY2EyMDk5LmNlcjAsBggrBgEFBQcwAYYgaHR0cDovL3BraWN2cy5jaXNj
by5jb20vcGtpL29jc3AwHwYDVR0jBBgwFoAUOJVXDzQjTvOhJiC6FJHHQYgdo1sw
UgYDVR0gBEswSTBHBgorBgEEAQkVAR4AMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93
d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy8wQwYDVR0fBDwwOjA4
oDagNIYyaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2NybC9jcmNh
MjA5OS5jcmwwHQYDVR0OBBYEFOpro7nBE5d+G/s6jWhgBzlfh0j6MA0GCSqGSIb3
DQEBCwUAA4IBAQBcqYEOgAHhGWKndwM901XX2Enh4hjXR5avDg7G/f6Tb9H509dt
QW+AeZGEghhwUrw1EeG79tHkncAe+m+64xMC1ttyI1RSyn8rBqQYkXnnCRbtF/Nw
pQe5fjvdeIFWJhUI16TOt/ZlkNnWnLsUU1alZmN+J/FhSr8VTJWGRM9gY8hefH8f
5U7LMiDXxsFVHB7R6KGNjvtawrl6W6RKp2dceGxEIIvMahgMWWHHiWOQAOtVrHuE
NEjYR/7klLLwdgQF/NNCA2z47pSfMFnBcr8779GqVIbBTpOP2E6+1pBrE2jBNNoc
uBG1fgvh1qtJUdBbTziAKNoCo4sted6PW2/U
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEITCCAwmgAwIBAgIKBgEgAwc2RDFGxTANBgkqhkiG9w0BAQsFADAxMR8wHQYD
VQQDExZIaWdoIEFzc3VyYW5jZSBTVURJIENBMQ4wDAYDVQQKEwVDaXNjbzAgFw0y
MjA4MDExMDEwMDhaGA8yMDk5MDgwOTIwNTgyNlowYjEoMCYGA1UEBRMfUElEOkMx
MjAwLTE2UC0yRyBTTjpEVFkyNjMxMDAxNTEOMAwGA1UEChMFQ2lzY28xETAPBgNV
BAsTCFRQTSBTVURJMRMwEQYDVQQDEwpMSUdIVFNBQkVSMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxHlUxYHK+BoQ3N7sL2u0Tgc3aJuJGnfJbrMHtow3
S8EmyyebeZpdWbfpn/zFH8TC3J9cr1NA4EvYi1Qli9ioSuBlLTjDujhAIPVqZnmy
cEDjDG0QI2xPYz+nL83ULkYWWTejarfz4jIPYb9po1veMavEqcEtBQHmPAlbzZyL
adRSrj32ph+XlnZ8BKU1BzXq52zcXsz2fICd0evw4O9f2LOMTvzMkn/i8dLx4gy1
oP95/EgJLgTydtpZyuA8TG9fy23qrWdJJzM+ZS+6cYrl20Eu7j5t5oN3IfAYxMwk
1MRaR+Ft5QWgK/ZBvAd3emelLB7K48h/nxKBLrtD6aobiQIDAQABo4IBBjCCAQIw
DgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAU6mujucET
l34b+zqNaGAHOV+HSPowgaEGA1UdEQSBmTCBlqBQBgorBgEEAQkVAwQCoEITQDFG
OTlBMDQ5Qzk1MjgxRjU1RjhBNjhBNzJFMjA0OURCQzgyOTAwNjREMjUzMjdEMUI3
RDkzQ0IxNDc3MzdBMTmgQgYJKwYBBAEJFQIDoDUTM0NoaXBJRD1Vd0lDQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQkh3PTAdBgNVHQ4EFgQUDyWO
Gy2I7j1nREZxpDmwbA5+hcQwDQYJKoZIhvcNAQELBQADggEBAA2KBFfaQf5kFaMJ
DJtGTyMNfu0hYjELDCwMK04iepo1w8bg9Rlb25LXYX+Rkk1/ZlIo3wLmRYNIddow
NQbJwt8Ch27kYyjnHcBWgz/M/DWOfKgEpNlS/Lw3ssLiAN67Y4dqUycUq7QVwG/I
zHO8oMu4sWjarkpiMTibJbw6w5PbJhd8meHoaJA1AV0pNKASvsIKoCZI1cRP/RFZ
dnRMM9LQUqeVob9hn5WRQ5PrweuALXMkUpmqeHsxSxa0M9w2u7dDYq/oeGZuUk93
9JaBqW4nwZ50MkwK9qLzYFzR5HD+YfJup22DoSdXZhO+gz4MzVCqDp5zsEyDPZl6
XLN5ZZ4=
-----END CERTIFICATE-----
```

Example 2: The following example displays the SUDI certificate chain with a signature over the certificates using a nonce of 12345:

```
switchxxxxxx> show platform sudi certificate sign nonce 12345
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a1lEb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30SecmrxkmQBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAyODA4WhgPMjA5OTA4MDkyMDU4MjdaMDExHzAdBgNVBAMTFkhpZ2ggQXNzdXJh
bmNlIFNVREkgQ0ExDjAMBgNVBAoTBUNpc2NvMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAvdzeSWdDI6lRZDYRvA6JqaRvQyy6Dx1WaqI82UeKR4ZRn0ef
xMGvp4c88/VMS8WSjQO1qolMfMxqHkcSiFBOULx6Trquw4TrEf9sIuzvgJvDaEa8
IllXPwtPtNqZEIWi8jlinz2uGam93KuGPcioHfruzbDKWHL/HWFGYMgz+OKwhD3J
4NRySknQvUovfV8eWLeVOqW8rbnG3TZxv5VexOiK4jL3ObvsQPuAWUwUoo7nuFlE
GTG/VCeyCe/H8+afIScbZOkI9xejtckflnBYFVCyFxzm2H3YZatb6ohbyRXLtOPj
T3SJ+OOoYMlSLd28z727LpRbFFLGYhyWxEXDuQIDAQABo4IBgjCCAX4wDgYDVR0P
AQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYBAf8CAQAwfwYIKwYBBQUHAQEEczBxMEEG
CCsGAQUFBzAChjVodHRwczovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2Nl
cnRzL2NyY2EyMDk5LmNlcjAsBggrBgEFBQcwAYYgaHR0cDovL3BraWN2cy5jaXNj
by5jb20vcGtpL29jc3AwHwYDVR0jBBgwFoAUOJVXDzQjTvOhJiC6FJHHQYgdo1sw
UgYDVR0gBEswSTBHBgorBgEEAQkVAR4AMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly93
d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9wb2xpY2llcy8wQwYDVR0fBDwwOjA4
oDagNIYyaHR0cDovL3d3dy5jaXNjby5jb20vc2VjdXJpdHkvcGtpL2NybC9jcmNh
MjA5OS5jcmwwHQYDVR0OBBYEFOpro7nBE5d+G/s6jWhgBzlfh0j6MA0GCSqGSIb3
DQEBCwUAA4IBAQBcqYEOgAHhGWKndwM901XX2Enh4hjXR5avDg7G/f6Tb9H509dt
QW+AeZGEghhwUrw1EeG79tHkncAe+m+64xMC1ttyI1RSyn8rBqQYkXnnCRbtF/Nw
pQe5fjvdeIFWJhUI16TOt/ZlkNnWnLsUU1alZmN+J/FhSr8VTJWGRM9gY8hefH8f
5U7LMiDXxsFVHB7R6KGNjvtawrl6W6RKp2dceGxEIIvMahgMWWHHiWOQAOtVrHuE
NEjYR/7klLLwdgQF/NNCA2z47pSfMFnBcr8779GqVIbBTpOP2E6+1pBrE2jBNNoc
uBG1fgvh1qtJUdBbTziAKNoCo4sted6PW2/U
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEITCCAwmgAwIBAgIKBgEgAwc2RDFGxTANBgkqhkiG9w0BAQsFADAxMR8wHQYD
VQQDExZIaWdoIEFzc3VyYW5jZSBTVURJIENBMQ4wDAYDVQQKEwVDaXNjbzAgFw0y
MjA4MDExMDEwMDhaGA8yMDk5MDgwOTIwNTgyNlowYjEoMCYGA1UEBRMfUElEOkMx
MjAwLTE2UC0yRyBTTjpEVFkyNjMxMDAxNTEOMAwGA1UEChMFQ2lzY28xETAPBgNV
BAsTCFRQTSBTVURJMRMwEQYDVQQDEwpMSUdIVFNBQkVSMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxHlUxYHK+BoQ3N7sL2u0Tgc3aJuJGnfJbrMHtow3
S8EmyyebeZpdWbfpn/zFH8TC3J9cr1NA4EvYi1Qli9ioSuBlLTjDujhAIPVqZnmy
cEDjDG0QI2xPYz+nL83ULkYWWTejarfz4jIPYb9po1veMavEqcEtBQHmPAlbzZyL
adRSrj32ph+XlnZ8BKU1BzXq52zcXsz2fICd0evw4O9f2LOMTvzMkn/i8dLx4gy1
oP95/EgJLgTydtpZyuA8TG9fy23qrWdJJzM+ZS+6cYrl20Eu7j5t5oN3IfAYxMwk
1MRaR+Ft5QWgK/ZBvAd3emelLB7K48h/nxKBLrtD6aobiQIDAQABo4IBBjCCAQIw
DgYDVR0PAQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAU6mujucET
l34b+zqNaGAHOV+HSPowgaEGA1UdEQSBmTCBlqBQBgorBgEEAQkVAwQCoEITQDFG
OTlBMDQ5Qzk1MjgxRjU1RjhBNjhBNzJFMjA0OURCQzgyOTAwNjREMjUzMjdEMUI3
RDkzQ0IxNDc3MzdBMTmgQgYJKwYBBAEJFQIDoDUTM0NoaXBJRD1Vd0lDQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQkh3PTAdBgNVHQ4EFgQUDyWO
Gy2I7j1nREZxpDmwbA5+hcQwDQYJKoZIhvcNAQELBQADggEBAA2KBFfaQf5kFaMJ
DJtGTyMNfu0hYjELDCwMK04iepo1w8bg9Rlb25LXYX+Rkk1/ZlIo3wLmRYNIddow
NQbJwt8Ch27kYyjnHcBWgz/M/DWOfKgEpNlS/Lw3ssLiAN67Y4dqUycUq7QVwG/I
zHO8oMu4sWjarkpiMTibJbw6w5PbJhd8meHoaJA1AV0pNKASvsIKoCZI1cRP/RFZ
dnRMM9LQUqeVob9hn5WRQ5PrweuALXMkUpmqeHsxSxa0M9w2u7dDYq/oeGZuUk93
9JaBqW4nwZ50MkwK9qLzYFzR5HD+YfJup22DoSdXZhO+gz4MzVCqDp5zsEyDPZl6
XLN5ZZ4=
-----END CERTIFICATE-----
Signature version: 1
Signature:
6ca45d415eace3b6cc09d84026dfcb4d1fbf614c319d3d28a3b924f6f432b26254aeca9c22aa150c
cfadd78bf2c4326d89f863eb52893e2cf3b9ddcd6d1f8ff00ea5830eec1281446c5ab5c92eee0030
6d25a1c75a6b0deaf9fee88b2b62d5e341bbe2fdbfb4cf4b5720d74f4e63f16c2012baadb5251a9d
bc871c4977335b8152715a95b48003d139e9e7e19fb7aa84f62e1a8c0e007a15f2a312c839b96170
e05e58a0e0f9ee78a28ffc9ddeb73fc7fdde0cbb556fa17aeb0d984bb4afa435fe40599de1c222bd
d132112ecb23ea1ca7ea78b40b2fb39d04867c05b0a7965e2180ba79688da06864be541f4956db96
3e48ad26f817bb56465f11e5ff89e128
```

Example 3: The following example displays the attestation (AIK) certificate chain with a signature over the certificates using a nonce of 67890:

```
switchxxxxxx> show platform attestation certificate sign nonce 67890
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5
MjA1ODI4WhgPMjA5OTA4MDkyMDU4MjhaMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYD
VQQDExJDaXNjbyBSb290IENBIDIwOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTtuM1fg0+9Gflik4axlCK1I2fb3ESCL8+tk8kOXlhfrJ/zlfRbe60
xRP0iUGMKWKBj0IvvWFf4AW/nyzCR8ujTt4a11Eb55SAKXbXYQ7L4YMg+lmZmg/I
v3GJEc3HCYU0BsY8g9LuLMvqwiNmAwM2jWzNq0EPArt/F6RiQKq6Ta3e7VIfDZ7J
65OA2xASA2FrSe9Vj97KpQReDcm6G7cqFH5f+CrdQ4qwAa4zWNyM3kOpUb637DNd
9m+n6WECyc/IUD+2e+yp21kBZIKH7JvDpu2U7NBPfr52mFX8AfCZgkXV69bp+iYf
saH1DvXIfPpNp93zGKUSXxEj4w881t2zAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIB
BjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQ4lVcPNCNO86EmILoUkcdBiB2j
WzANBgkqhkiG9w0BAQsFAAOCAQEAjeKZo+4xd05TFtq99nKnWA0J+DmydBOnPMwY
lDrKfBKe2wVu5AJMvRjgJIoY/CHVPaCOWH58UTqfji95eUaryQ/s36RKrBgMMlwr
WNItxE625PHuaN6EjD1WdWiRMZ2hy8F4FCKz5hgUEvN+PUNZwsPnpU6q3Ay0+11T
4TriwCV8kJx3cWu0NvTypYCCXMscSfLFQR13bo+1z6XNm30SecmrxkmQBVMqjCZM
VvAxhxW1iGnYdPRQuNqt0xITzCSERqg3QVVqYnFJUkNVN6j0dmmMVKZh17HgqLnF
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEXzCCA0egAwIBAgIJCsCKA1bCuHJDMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODEx
MjAzMjQyWhgPMjA5OTA4MDkyMDU4MjdaMCkxFzAVBgNVBAMTDkF0dGVzdGF0aW9u
IENBMQ4wDAYDVQQKEwVDaXNjbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAPH9/H1Cno5OxJ7xqpZZmnnfuuHKhhXQTjz6dUkjmbJmUXsFHMCNikbkLgTj
qgsbSfeOG0kVFAJCC2XkMsWgjuLV8laHXAY/tRWrgyHJ7RkqqUTh7ZLmhNFPxQaj
DdaqaPDNyKplgl8KhXwF+n1n4PQuH45dUE3Tp4P80AVZ4fNmow5n409ZIpcjOYfS
iLiQ8fID9hhY3GAVh5ugfLbLKhojCojCNgT+gzR4IM6amzHku1Ysuf7mUFd8vJtd
AWekGtr1XUB2gJ72vXwqV0lf4uFw7GHO+hREqogRLhtF/7uH6CoVO/fmcUFYIT+C
MSKzxJAbeITSd13WCNzSXYiXrTMCAwEAAaOCAYIwggF+MA4GA1UdDwEB/wQEAwIB
BjASBgNVHRMBAf8ECDAGAQH/AgEAMH8GCCsGAQUFBwEBBHMwcTBBBggrBgEFBQcw
AoY1aHR0cHM6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3braS9jZXJ0cy9jcmNh
MjA5OS5jZXIwLAYIKwYBBQUHMAGGIGh0dHA6Ly9wa2ljdnMuY2lzY28uY29tL3Br
aS9vY3NwMB8GA1UdIwQYMBaAFDiVVw80I07zoSYguhSRx0GIHaNbMFIGA1UdIARL
MEkwRwYKKwYBBAEJFQEcADA5MDcGCCsGAQUFBwIBFitodHRwOi8vd3d3LmNpc2Nv
LmNvbS9zZWN1cml0eS9wa2kvcG9saWNpZXMvMEMGA1UdHwQ8MDowOKA2oDSGMmh0
dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3braS9jcmwvY3JjYTIwOTkuY3Js
MB0GA1UdDgQWBBQAHroP19nnPZCyDOSo7cfzLETspjANBgkqhkiG9w0BAQsFAAOC
AQEAhyXlbLYZRW6CxRvVobb4Gvt8HFHKCaqx0yPbnDAjktzq3/yrb6TevdITFt2U
VZjO78/yJRACGffz8dlaBnVp8LEMcBZTzs2tvP6gkjgptqC+FFV0+8lCdxzoeRx6
vaVgpd9CPbpfLRp4wewp/phXonRshNxWXdVgk2lK/o3njguc/5jI5SPzejFMMJOF
ZgrExhmcKRDVap9fJi/JOizO+1Qwp9hPEthBElv9UksA4NKEdiwNjTOhPB6GU7wU
XrSFE5Svf5YVAPxKl0Gkw5ulSTiWM7UsnS1RaXfBPqrsR1SlzIQQlr4B85EzTBuK
HvlCRCEPQZcg3CItn3b8UtPLLQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEGTCCAwGgAwIBAgIKA4Nld5RVSDU2ozANBgkqhkiG9w0BAQsFADApMRcwFQYD
VQQDEw5BdHRlc3RhdGlvbiBDQTEOMAwGA1UEChMFQ2lzY28wIBcNMjIwODAxMTAx
MDA4WhgPMjA5OTA4MDkyMDU4MjZaMGIxKDAmBgNVBAUTH1BJRDpDMTIwMC0xNlAt
MkcgU046RFRZMjYzMTAwMTUxDjAMBgNVBAoTBUNpc2NvMREwDwYDVQQLEwhUUE0g
U1VESTETMBEGA1UEAxMKTElHSFRTQUJFUjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAJtUHXzPGFhzrlJ251GUrGuL8Ek3axTdrurLqzNslvkx5Ystp2VM
Q5qDua2ovRcESrSxTfNMwUDm9+FX8EipsxgIRX5+oZZ8ka8oNVEKyTPyB5upl7Xi
9G15wvVBUHceVERCX33LqV2wHiA2hMdsgDsSeGlJteQi3zjeokXeojW9MDyJsMTp
CBQHCGNS+GgKXSqMt3k54K8S3RSi/P/R/oPKoA0z2ZUsu9/bOHTAwX/ZGMJ8U48X
C93adaOef1J0grt5scL073jZ1SbI4NS2ind8DGS2f059pdKHZvCetNJMcGugnapx
S6jOkf4qiTVSpbuEos8VDMgubaWf7KUUSB8CAwEAAaOCAQYwggECMA4GA1UdDwEB
/wQEAwIF4DAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFAAeug/X2ec9kLIM5Kjt
x/MsROymMIGhBgNVHREEgZkwgZagUAYKKwYBBAEJFQMEAqBCE0AxRjk5QTA0OUM5
NTI4MUY1NUY4QTY4QTcyRTIwNDlEQkM4MjkwMDY0RDI1MzI3RDFCN0Q5M0NCMTQ3
NzM3QTE5oEIGCSsGAQQBCRUCA6A1EzNDaGlwSUQ9VXdJQ0FBQUFBQUFBQUFBQUFB
QUFBQUFBQUFBQUFBQUFBQUFBQUJIdz0wHQYDVR0OBBYEFC2RwVIJl3l6EDvF
+2jc19Vq6mIdMA0GCSqGSIb3DQEBCwUAA4IBAQB0U1fS7UQaHdkhB/X44U+fOt0U
```

```
1wW/L5yPuDc7zWGHcxFkdZBP+4e4M491dKI8B0ULdFhZThHNf/WeQ2c9TftPc0kI
f3gqo9ez7oBlM/2Y1luG0D3WigAyZjonqmW3/tikYiVKGs7eGGylO22S9y5jXxjz
qqtz5LU+S9d18NGtKD1rYhA12ZZ9ikUhBUPDpbG0JanGaYOLpwVl7wkynYnI5bhn
gjAylgV5RqBRN6luvDWTN02LvXCKYChSMJxH8VN8d75D68qg/XcL0zcTUVViENsi
grZkZxpqU3cRJqSUVBsPXSSKhgryuVv0wcZcMAU1Bg7elM67bTzet+d1YvWH
-----END CERTIFICATE-----
Signature version: 2
Signature:
33bf4ff78bf66930494bc2376244e9b022931b7c0519a5d123e5571287a5b1ddcc4b90a80870d263
ec9f5a38b9f4c44973527b4ddcb6c8d515e64c9862362884671fff7e1e279fa6d1d8b3d81604930a
0a94b6ba8f6224ce6b60172b105ced211120528af39362269f0b4bbf7adcc9532e108b4035d2d139
62ffd5792ac1565f7e04932938b942e90ca9aefb8bf4a3cd0f804494486e1b579934aac8f42a57e9
40069463151d5e01c1d5e8b8e66b4f300c05e01aadcfaf3dc0588b6e699f1367af4fcfe19bc58a21
55d02592a7fbe158558937b9c642d90c39ce9f7a8f759cc8ec230443410dd668f3a9383bc89cc546
650902fbc637f921b4a3d17007ee98bb
```

show platform hardware integrity

Use the show platform hardware integrity Privileged EXEC mode command to display chip protection information, including the content of PCR-15 (PCR - Platform Configuration Register) of the Active unit, and optionally a signature over the PCR or the PCR Quote included in command output display.

Syntax

show platform hardware integrity [[attestation] [sign [nonce <nonce>]]]

Parameters

- **sign**—(Optional) display a signature over PCR-15 or PCR-15 Quote.
- **attestation** - (Optional) use the attestation (AIK) private key to sign the PCR-15 Quote. If the attestation is not specified then the SUDI private key is used to sign PCR-15.
- [**nonce** <nonce value>]—(Optional) provide a nonce to use with the signature to protect from replay attacks. (range 0-4,294,967,295)

Default Usage

PCR information is displayed without a signature. If the sign keyword is specified without a nonce value then the signature will be generated without using a nonce. If the attestation keyword is not specified then the SUDI private key will be used to sign the PCR.

Command Mode

Privileged EXEC mode

User Guidelines

The **show platform hardware integrity** command provides on demand chip protection attestation. The command displays the content of the Active unit PCR (Platform Configuration Register) 15. PCR-15 is the extension of the device unique chip IDs. If the **sign** keyword is used, then the command output will display a signature over PCR-15. If the **attestation** keyword is used then the command output will include also a PCR Quote and the signature will be over the quote.

The command also supports an optional [**nonce** <nonce value>] parameter used as part of the signature inputs to prevent replay attacks. If the [**nonce** <nonce value>] parameter is not provided the signed data will not include the nonce.

The command output includes a signature version. A signature value of 1 indicates that the SUDI private key was used for signing PCR-15. A signature value of 2 indicates that the attestation (AIK) private key was used for signing the PCR Quote.

Examples

Example 1: The following example displays the contents of PCR-15 without a signature:

```
switchxxxxxx> show platform hardware integrity
PCR15: b45f34da34c6b142569f2c4f36264f3d0dfadde33f7721ed4bfd7b329ec71e6c
```

Example 2: The following example displays PCR-15 with a signature over PCR-15 using the SUDI private key with no nonce:

```
switchxxxxxx> show platform hardware integrity sign
PCR15: b45f34da34c6b142569f2c4f36264f3d0dfadde33f7721ed4bfd7b329ec71e6c
Signature Version: 1
Signature:
aba857b3c4a00191d6bc01617b5e73755810f0f4f67230e96de7a305f6882d94da9bdd2df3f12472
33f42fe0137b11971c128252e3a9813ec78d8640d87f284fc427db96b3412a07c24c78cda2242bd5
96c69ea06beb28feabfa014c48b96f420d65ffa725221319791e1f7c094acf743bbd48b7aafe088b
147894de42ca0e0634155432d8092b0ca82eb246ddb2de9a0bbd9a7914fdd7a1628dd5a29bbc4d02
9ddf846938e0b47f63bc488cf3dd2f439e684989ff39e834ac7534f5bc2187b293cfc5445af9a905
c8a3a5366fbc2cd74868912105ef4880a203772946ffae2de126cd769d111b362210bb9ce7a2af7b
f423360a90ac8dde4aacc2b47a7cc923
```

Example 3: The following example displays PCR-15, PCR-15 Quote and the signature over the quote using the attestation (AIK) key with a nonce of 613:

```
switchxxxxxx> show platform hardware integrity sign attestation nonce 613
PCR15: b45f34da34c6b142569f2c4f36264f3d0dfadde33f7721ed4bfd7b329ec71e6c
Signature Version: 2
Quote:
ff544347801800220000b9f2c580f14cf6f157964c1dc9fb17f8a9504b50976a120fb870831db9242
e5ac00207e5fab8920a8bbcd214d7ade666c74fc07f2aa41298ac81177dc9ba7f5af978100000000
002be9b5000000240000000001000201100000000000000001000b030080000020f508f73aab654d
716ae4a511616843ca53bdef8bb7959a26226dd4d477e7170b
Signature:
36e4f4d5fecaa820cd9dfb879b170007e35eeb2edb1ddb9736580c3bd7aefc1312e6bb946573b8ef
45b9f97084b1648c704d4e54ff6aa854e2ebd4389c880b2c060be391e14d14a411cc675fe6cde688
cf3d688570eaf5bd08b69185f7dfcbbe2a5329939096aa47b0bea5fc0f1907029789f67fbb187d88
2dc69bf24dda351fc55846be38d233d40a164f30a82482f72733c9c33decb06376527034ab19490b
fccbd8f4e108910fa0a923047f98e8c45ba9d9d8e28d134662c52d6ed5616d6fc33e40985b6c3921
644d3e53570c5bc17a7f4289cd46fb3f72a7e440720751889a2552395e9ef66ba9a6d8fe9b9a6aeb
a74e43129fa5447ad9b7158401cd9174
```

show platform integrity

Use the show platform integrity Privileged EXEC mode command to display Boot Integrity Visibility (BIV) information for the Active unit, and optionally a signature over the PCR or the PCR Quote included in command output display.

Syntax

show platform integrity [sign [attestation] [nonce <nonce>]]

Parameters

- **sign**—(Optional) display a signature over the PCRs displayed in the command output or over the PCR Quote displayed in the command output.
- **attestation**—(Optional) use the attestation (AIK) private key to sign the PCR Quote. If the **attestation** is not specified then the SUDI private key is used to sign the PCRs.
- [**nonce** <nonce value>]—(Optional) provide a nonce to use with the signature to protect from replay attacks. (range 0-4,294,967,295)

Default Usage

PCR information is displayed without a signature. If the sign keyword is specified without a nonce value then the signature will be generated without using a nonce. If the attestation keyword is not specified then the SUDI private key will be used to sign the PCRs.

Command Mode

Privileged EXEC mode

User Guidelines

The **show platform integrity** command provides on demand Boot Integrity Visibility (BIV) attestation. The command displays the boot-up measurements of the Active unit boot-loader image and OS image. The measurements are displayed as hash values. In addition, the command output displays the contents of PCR-0 and PCR-8. PCR-0 is the extension of the boot-loader image hash, and PCR-8 is the extension of the OS image hash. If the **sign** keyword is used, then the command output will display a signature over PCR-0 and PCR-8. If the **attestation** keyword is used then the command output will include also a PCR Quote and the signature will be over the quote.

The command also supports an optional [**nonce** <*nonce value*>] parameter used as part of the signature inputs to prevent replay attacks. If the [**nonce** <*nonce value*>] parameter is not provided the signed data will not include the nonce.

The command output includes a signature version. Signature value of 1 indicates that the SUDI private key was used for signing PCR-0 and PCR-8, while a signature value of 2 indicates that the attestation (AIK) private key was used for signing the PCR Quote.

Examples

Example 1: The following example displays the measurements of the images and the contents of PCR-0 and PCR-8 without a signature:

```
switchxxxxxx> show platform integrity
Platform: C1300-48P-4X
Boot Loader Version: 1.0.74
Boot Loader Hash:
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5
OS Version: 4.0.0.76
OS Hash: 26F68EE9341A4CBB552D1A3D9B02920DF126287F12EEEADFC47BD0A8EE8B7D04
PCR0: ca153e2fddadb6af4b08721421c336d874f0a950c7f9699c1509a5fcb86017d6
PCR8: 9c26a9a7ca8033bb050df2b6974cbe0d3f17d65302feb637b40a37aff976e8b9
```

Example 2: The following example displays the measurements of the images and the contents of PCR-0 and PCR-8 with a signature over PCR-0 and PCR-8 using the SUDI private key and a nonce value of 248:

```
switchxxxxxx> show platform integrity sign nonce 248
Platform: C1300-48P-4X
Boot Loader Version: 1.0.74
Boot Loader Hash:
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5
OS Version: 4.0.0.76
OS Hash: 26F68EE9341A4CBB552D1A3D9B02920DF126287F12EEEADFC47BD0A8EE8B7D04
PCR0: ca153e2fddadb6af4b08721421c336d874f0a950c7f9699c1509a5fcb86017d6
PCR8: 9c26a9a7ca8033bb050df2b6974cbe0d3f17d65302feb637b40a37aff976e8b9
Signature Version: 1
Signature:
74c2795731dad3fd9cb35310e3d3070dc666ec0ced60ad1b4586f08c18a7d6f5c82db6ac755794ca
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5cac3d89
838696745bfbc620a95523574c6cc6128fbfcbaf86df88d5f56bda32d9f82f3b10ca8d170eac17f0
526194afd80c7880f8074de85eb81777bc94a6ef748f04737bb1ed29debb2d1c0a71074e8e4513b6
ba9253460c205cdd641bfe7976d16d13857db0115a9efd427ce0ccd86c1832b6ad3408640fec4a6f
ca40baebca3a0e2ab395774223776ebebc279e7ec7c759e949fee756f47cb6ca6c326edf68a35444
33f3ef8befcaac78b631188204191745
```

Example 3: The following example displays the measurements of the images, the contents of PCR-0 and PCR-8, a PCR Quote and a signature over the quote using the attestation (AIK) key and a nonce value of 365:

```
switchxxxxxx> show platform integrity sign attestation nonce 365
Platform: C1300-48P-4X
Boot Loader Version: 1.0.74
Boot Loader Hash:
810ca3abed75aec7fe3aeb5baa452e7577d2cd15970dae948368f23ee17575b2ae47701e5
OS Version: 4.0.0.76
OS Hash: 26F68EE9341A4CBB552D1A3D9B02920DF126287F12EEEADFC47BD0A8EE8B7D04
PCR0: ca153e2fddadb6af4b08721421c336d874f0a950c7f9699c1509a5fcb86017d6
PCR8: 9c26a9a7ca8033bb050df2b6974cbe0d3f17d65302feb637b40a37aff976e8b9
Signature Version: 2
Quote:
ff54434780180022000b9f2c580f14cf6f157964c1dc9fb17f8a9504b50976a120fb870831db9242
e5ac000800000000000016d00000000002d085b0000002400000000010002011000000000000000
01000b0301010000200bf8a79c7d864c5556976737edc9a8e870e767d371cf6239892401f76e377e
64
Signature:
14d9b51c83185e790d6485ca76d58bfaab925ba0bc1f1a5ea4590d244b5206c69f53c84d8fc6d715
3af67ab747c7aebd3ba81bf36fbb11e45097adbcd6ec2d924496165505c52dc6a77c386156188e9e
0ce03d58cdbe1babe45141760a8b965440a82af1d3751e9f0b8e8570564c416a407fee901c175594
b7b2a556985c8df924b576f9d898e84db344af19aa724b20f5832d18c1ba2b0c501ef57670dfa643
31970179ea8415aaf2424abdf197386a8b6018c75f2346b930c982eba309aef350075812b894c2ac
36af9594d0d27b0c9aab0e6be17575ba1fc90d898cf70ed6e0a1ccdb15592b9ba8f08d6fb98f70a2
33905b820c64c08247e5ea2a81849b11
```

show reload

To display whether there is a pending reload for status of the device, use the **show reload** Privileged EXEC mode command.

Syntax

show reload

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

You can use this command to display a pending software reload. To cancel a pending reload, use this command with the **cancel** parameter.

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)
```

show sessions

To display open Telnet sessions, use the **show sessions** User EXEC mode command.

Syntax

show sessions

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User 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.

show software versions

To display system software version information use the following, **show software versions** Privileged EXEC mode command.

Syntax

show software versions [unit *unit-id***] [detailed]**

Parameters

- **Detailed** - (optional) Display additional software version also related to BootRom booton, CPLD, PoE controller, OpenSSH and OpenSSL.

Defaults

Displays the following software version info - image, bootloader and kernel.

Command Mode

Privileged EXEC mode

User Guidelines

The **show software versions** command displays the version information of device image, BootRom, booton, bootloader and kernel as well as relevant software modules.

Examples

Example 1: The following example displays basic device software version information:

```
switchxxxxxx# show software versions
```

Active-image version:	1.2.3.4
In-active-image version:	5.6.7.8 (active after reboot)
Kernel version:	Linux 3.10.70

Unit 1 Bootloader version:	U-Boot 2013.01 (Sep 02 2018 - 00:32:52)

Example 2: The following example displays detailed device software version information

```
switchxxxxxx# show software versions detailed
```

Active-image version:	1.2.3.4
In-active-image version:	5.6.7.8 (active after reboot)
Kernel version:	Linux 3.10.70
OpenSSL version:	1.1.0b
OpenSSH version:	7.3p1
BootRom version:	1.20
Booton version:	6.13
Bootloader version:	U-Boot 2013.01 (Sep 02 2018 - 00:32:52)
CPLD version:	9.29
PoE controller version:	21.190.18.3

show system

Use the **show system** User EXEC mode command to display system information.

Syntax

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

Parameters

unit-id—Specifies the unit number. (Range: 1 – 4)

Command Mode

User EXEC mode

User Guidelines

Use the **show system** command to display system information.

The *System MAC address* output displays device base MAC address (not configurable by user).

The *System Object ID* output displays the unique System Object ID (not configurable by user).

The *fan* output displays, per each unit, the device fan(s) status summary. The value of fail indicates that one or more of the fans is not functioning properly. To view specific status per each fan in device use the command show system fans, on page 1179.
The *sensor* and *temperature* output displays, per each unit, the temperature level and general status of all sensors. The value of fail for sensors indicates one ore more sensors are

```
not functioning propery. To view per sensor status, temperature read and threshold levels,
 use command show system sensors, on page 1181.
```

Example 1: The following example displays system information of a stack .

```
switchxxxxxx# show system
System Description:                    C1300-48P-4X
System Up Time (days,hour:min:sec):    03,02:27:46
System Contact:
System Name:                           switch151400
System Location:
System MAC Address:                    00:24:ab:15:14:00
System Object ID:                         1.3.6.1.4.1.9.6.1.1006.48.5
Unit        Type
---- -----------------
1          C1300-48P-4X
2          C1300-48P-4X
Unit Fans Status
---- -----------
1        OK
2        fail
Unit     Sensor Status             Temperature Level
---- --------------------- -------------------------
1             OK                    Warning
2             Fail                  Warning
```

Example 2: The following examples displays system information for unit 2 in a stack.

```
switchxxxxxx# show system unit 2
System Description:                          xxxx
System Up Time (days,hour:min:sec):  08,23:03:46
System Contact:
System Name:
System Location:
System MAC Address:                   00:99:88:66:33:33
System Object ID:                     1.3.6.1.4.1.674.10895.3031
Fans Status:                            OK
#Editor: For systems with no temperature sensors, the temperature in the following line
will be blank and the Status will be N/A
Unit    Sensor Status               Temperature Level
----   ---------------------    -------------------------
2             Fail                    Critical
```

show system languages

To display the list of supported languages, use the **show system languages** User EXEC mode command.

Syntax

show system languages

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays the languages configured on the device. Number of Sections indicates the number of languages permitted on the device.

```
switchxxxxxx> show system languages
 Language Name   Unicode Name   Code
--------------- -------------- ------
    English         English     en-US
   Japanese       µùÑµ£¼F¬P    ja-JP
```

show system tcam utilization

To display the Ternary Content Addressable Memory (TCAM) utilization, use the **show system tcam utilization** EXEC mode command.

Syntax

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

Parameters

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

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays TCAM utilization information.

switchxxxxxx> **show system tcam utilization**

```
System: 75%

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

show services tcp-udp

To display information about the active TCP and UDP services, use the **show services tcp-udp** Privileged EXEC mode command.

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
UDP6 A ll-161             SNMP
```

show tech-support

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

Syntax

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

Parameters

- **memory**—(Optional) Displays memory and processor state data.
- **config**—(Optional) 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

User 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**

show system fans

To view the status of the fans on the device, use the **show system fans** User EXEC mode command.

Syntax

show system fans [*unit-id*]

Parameters

unit-id—(Optional) Specifies the unit number to be reloaded. (Range: 1 – 4). If unspecified, displays information for all the units.

Command Mode

User EXEC mode

User Guidelines

Use the **show system fans** command to display detailed information per fan. The following information will be displayed:

- Per fan actual RPM.
- Per fan status - Possible values are: OK, fail; read fail; .

Examples

Display for units whose hardware supports variable fan speed.

```
switchxxxxxx> show system fans
```

Unit ID: 1		
Unit/fan ID ==========	Fan Actual Speed (RPM) =====	Fan Status ========
1/1	6000	OK
1/2	NA	Fail
1/3	NA	Read fail
1/4	4000	OK

Unit ID: 2		
Unit/fan ID ==========	Fan Actual Speed (RPM) =====	Fan Status ========
2/1	8000	OK
2/2	8000	OK
2/3	8000	OK

Unit ID: 3		
Unit/fan ID ==========	Fan Actual Speed (RPM) =====	Fan Status ========
3/1	5000	OK
3/2	4500	OK
3/3	5000	OK

Display for devices that do not support display of fan speed:

```
switchxxxxxx> show system fans
```

Unit ID: 1

Unit/fan ID =========	Fan Status ========
1/1	OK
1/2	Fail
1/3	Read fail
1/4	OK

Unit ID: 2	
Unit/fan ID =========	Fan Status ========
2/1	OK
2/2	OK
2/3	OK

Unit ID: 3	
Unit/fan ID =========	Fan Status ========
3/1	OK
3/2	OK
3/3	OK

show system sensors

To view the temperature sensor status, use the **show system sensors** User EXEC mode command.

Syntax

show system sensors

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

User Guidelines

Use the **show system sensors** command to display detailed sensor information , per each device sensor. Information is displayed per each unit in the stack.

The following information will be displayed:

- Sensor status.
- Sensor temperature reading
- Warning and Critical Alarm thresholds (temperature in Celsius)
- Location of specific sensor. Possible locations are: PP (Packet processor sensor); PCB (Sensor located on the Printed board circuit); PHY (PHY sensor); POE (Poe chip sensor).

Examples

Display for Stack systems with multiple sensor statuses

```
switchxxxxxx> show system sensors
```

Unit/ Sensor ======	Sensor status ======	Temperature (C) ==========	Warning Alarm Temp (C) ==========	Critical Alarm Temp (C) ==========	Sensor Location ======
1/1	OK	44	50	65	PCB
1/2	Failure	NA	65	75	PP
2/1	OK	65	60	70	PHY

show system id

To display the system identity information, use the **show system id** User EXEC mode command.

Syntax

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

Parameters

unit *unit-id*—(Optional) Unit number or all. If unspecified, defaults to all. (Range: 1 – 4)

Command Mode

User EXEC mode

Example

The following example displays the system identity information.

```
switchxxxxxx> show system id
serial number 114
```

show ports leds configuration

To display whether the LEDs of the ports are enabled or disabled, use the **show port leds configuration** User EXEC mode

command.

Syntax

show ports leds configuration

Parameters

This command has no arguments or keywords.

Command Mode

User EXEC mode

Example 1: The following example displays the status of the port's LEDs when they are turned on.

```
switchxxxxxx> show ports leds configuration
Port leds are not disabled
x
```

Example 2: The following example displays the status of the port LEDs when they are turned off.

```
switchxxxxxx> show port leds configuration
Port leds are disabled
```

show users

To display information about the active users, use the **show users** User EXEC mode command.

Syntax

show users

Parameters

This command has no arguments or keywords.

Default Usage

None

Command Mode

User EXEC mode

Example

The following example displays information about the active users.

```
switchxxxxxx> show users

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

show hardware version

To display hardware version information, use the **show hardware version** User EXEC mode command.

Syntax

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

Parameters

- ***unit***—(Optional) Specifies the unit number. (Range: 1 – 4)

Default Usage

Show hardware version on all units if no unit is specified.

Command Mode

User EXEC mode

Example

The following example displays hardware version information.

```
switchxxxxxx> show hardware version
Unit   HW Version
----   ------------
1       1.0.0
2       1.0.0.
```

show hardware components

To display device hardware component information, use the **show hardware components** Privileged EXEC mode command.

Syntax

show hardware components

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

User Guidelines

The **show hardware components** command displays information for device components such as packet processor(s), CPU, flash, PHYs and other hardware components.

The information displayed per each component depends on the information available for that component. Example for information that is displayed: vendor name, manufacturing part number (MPN), and HW reversion.

Examples

Example 1: The following example displays information on device hardware components:

```
switchxxxxxx# show hardware components
```

```
MAC info:
```

Unit ID/ MAC ID ----------	Vendor -------	MPN ----	Revision ---------
1	Marvell	98DX3236	A0
2	Marvell	98DX3336	A0

```
CPU info:
```

Unit ID --------	Vendor --------	MPN ----
1	Marvell	88F6820 (Armada ARMv7)
2	Marvell	MV78230

```
PHY info:
```

Unit ID/PHY ID ----------	Vendor -------	MPN ----	Revision ---------
1	Marvell	88E1680	A0
2	Marvell	88E3222	NS
2/1	Marvell	88E3680	A0

```
Flash info:
```

Unit ID -------	Vendor ------	MPN ----
1	Micron	JS28F640J3D-75 (65536 Kbytes)
2	MXIC Macronix	MX30LF2G18AC-TI (65536 Kbytes)

system light

To light the networks port LEDs of a device, or of a specific unit in stack, use the **system light** EXEC mode command.

Syntax

system light [***unit*** *unit-id] [**duration** seconds*]

system light stop

Parameters

- **unit-id**—Specify unit number or if left blank, all will light up.
- **duration** *seconds*—The number of seconds to light the LEDs. If unspecified, defaults to 60 seconds. (Range: 5–3600)
- **stop**—Stop lighting the LEDs.

Command Mode

User EXEC mode

Example

The following example lights the system LED for 6 seconds.

```
switchxxxxxx> system light duration 65
```

system recovery

To set the system to automatically recover from temperature that reached the critical threshold, use the **system recovery** Global Configuration mode command.

To return to disable automatic recovery, use the **no** form of the command.

Syntax

system recovery

no system recovery

Parameters

This command has no arguments or keywords.

Default Configuration

System recovery is enabled by default.

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# no system recovery
```

system reset-button disable

Use the system reset-button disable Global Configuration mode command to disable the reset functionality of the device reset button. To re-enable the reset button functionality use the no form of the command.

Syntax

system reset-button disable

no system reset-button disable

Parameters

This command has no arguments or keywords.

Default Configuration

By default the device reset button functionality is enabled.

Command Mode

Global Configuration mode

User Guidelines

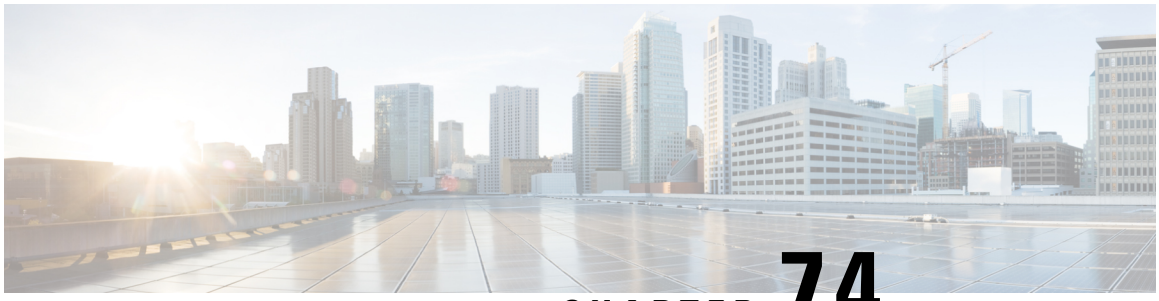
Use the system reset-button disable command to disable the reset functionality of the device reset button. When this command is applied the device will not reload or reset to factory default even if the reset button is pressed. This is useful to prevent unwanted device reload or setting to factory defaults due to accidental pressing of the button. The command disables the functionality of the reset button on all of the units in a stack.

If the reset button has other functionalities, besides reload and reset to factory default, they will not be effected by this setting.

Use the no form of command to re-activate the reset button and allow device reload and reset to factory default by pressing the button.

Examples

```
switchxxxxxx(config)# system reset-button disable
```



CHAPTER 74

TACACS+ Commands

This chapter contains the following sections:

- tacacs-server host, on page 1189
- tacacs-server host source-interface, on page 1190
- tacacs-server host source-interface-ipv6, on page 1191
- tacacs-server key, on page 1192
- tacacs-server timeout, on page 1193
- show tacacs, on page 1193
- show tacacs key, on page 1194

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** Global Configuration mode command. To delete the specified TACACS+ host, use the **no** form of this command.

Syntax

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**priority** *priority*]

encrypted tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *encrypted-key-string*] [**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**—(Optional) 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*—(Optional) 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*—(Optional) Specifies the timeout value in seconds. (Range: 1-30)
- **key** *key-string*—(Optional) 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 will be used.
- **key** *encrypted-key-string*—(Optional) Same as key-string, but the key is in encrypted format.
- **priority** *priority*—(Optional) 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 the **tacacs-server timeout** command) is used.

If **key-string** is not specified, the global value (set in the **tacacs-server key** command) 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
```

tacacs-server host source-interface

To specify the source interface which IPv4 address will be used as the Source IPv4 address for communication with IPv4 TACACS+ servers, use the **tacacs-server host source-interface** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

tacacs-server host source-interface *interface-id*

no tacacs-server host source-interface

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 TACACS+ server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# tacacs-server host source-interface vlan 100
```

tacacs-server host source-interface-ipv6

To specify the source interface whose IPv6 address will be used as the Source IPv6 address for communication with IPv6 TACACS+ servers, use the **tacacs-server host source-interface-ipv6** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

tacacs-server host source-interface-ipv6 *interface-id*

no tacacs-server host source-interface-ipv6

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 TACACS+ server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# tacacs-server host source-interface-ipv6 vlan 100
```

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the device and the TACACS+ daemon, use the **tacacs-server key** Global Configuration mode command. To disable the key, use the **no** form of this command.

Syntax

tacacs-server key *key-string*

encrypted tacacs-server key *encrypted-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)
- ***encrypted-key-string***—Same as key-string, but the key is in encrypted format.

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
```

tacacs-server timeout

To set the interval during which the device waits for a TACACS+ server to reply, use the **tacacs-server timeout** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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
```

show tacacs

To display configuration and statistical information for a TACACS+ server, use the **show tacacs** Privileged EXEC mode command.

Syntax

show tacacs [*ip-address*]

Parameters

- ***ip-address***—Specifies the TACACS+ server name, IPv4 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 Priority

Connection Out

--- --- --- --- --- ---

172.16.1.1 Connected 49 No Global 1

```
Global values
-------------
Time Out: 3
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

show tacacs key

To display the configured key of the TACACS+ server, use the **show tacacs key** Privileged EXEC mode command.

Syntax

show tacacs key [*ip-address*]

Parameters

- ***ip-address***—Specifies the TACACS+ server name or IP address.

Default Configuration

If *ip-address* is not specified, information for all TACACS+ servers is displayed.

Command Mode

Privileged EXEC mode

Example

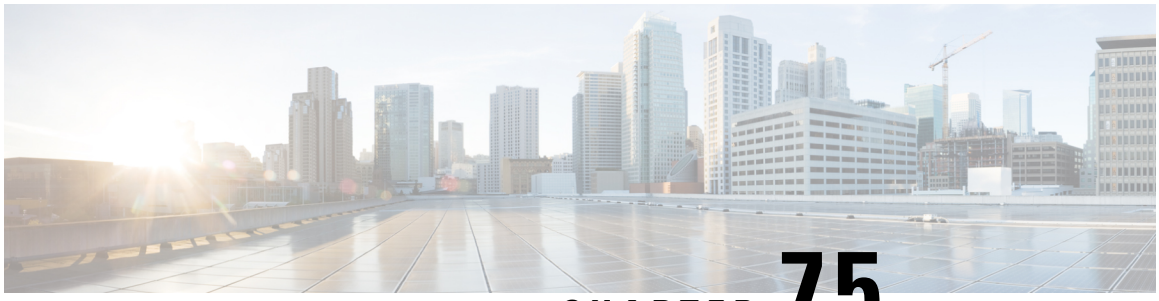
The following example displays configuration and statistical information for all TACACS+ servers.

```
switchxxxxxx# show tacacs key
```

IP address	Key (Encrypted)
----------	---------------
172.16.1.1	1238af77aaca17568f1298cced165fec
172.16.1.2	1238af77aaca17568f12988601fcabed

Global key (Encrypted)

1238af77aaca17568f1298bc5476ddad



CHAPTER 75

Telnet, SSH and Slogin Commands

This chapter contains the following sections:

- ip telnet server, on page 1195
- ip SSH logging, on page 1196
- ip ssh server, on page 1197
- ip ssh server algorithm, on page 1197
- ip ssh port, on page 1199
- ip ssh password-auth, on page 1200
- ip ssh pubkey-auth, on page 1200
- crypto key pubkey-chain ssh, on page 1201
- user-key, on page 1202
- key-string, on page 1203
- show ip ssh, on page 1204
- show crypto key pubkey-chain ssh, on page 1205

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

Disabled

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 an SSH server, use the **ip ssh server** command.

Example

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

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

ip SSH logging

To enable or disable sending traps related to SSH session setup and shutdown use the ip ssh logging in Global Configuration mode. To restore default setting, use the no form of this command.

Syntax

ip ssh logging [enable | disable]

no ip ssh logging

Parameters

- **enable** - Enables SSH logging on device
- **disable** - Disables SSH logging on device

Default Configuration

SSH session logging is disabled by default.

Command Mode

Global configuration mode.

User Guidelines

This command enables SSH logging on the device. SSH logging is a mean to track the progress of SSH session setup and tear-down. SSH session setup and tear-down progress is tracked using SYSLOG message which are generated as part of the process. If SSH logging is disabled then SYSLOG messages will not be generated as part of the SSH setup or tear-down process.

Example

The following example enables SSH logging on the device.

```
switchxxxxxx(config)# ip ssh logging enable
```

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 an SSH server, generates the encryption keys automatically.

To generate new SSH server keys, use the **crypto key generate dsa** and **crypto key generate rsa** commands.

Example

The following example enables configuring the device to be an SSH server.

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

ip ssh server algorithm

To enable one or more of the alogrithms used for the SSH session encryption, host-key key exchange (kex) or MAC, use the ip ssh server algorithm command in Global Configuration mode. To disable one or more of the SSH alogorithm, use the no form of this command.

Syntax

ip ssh server algorithm {encryption enc-alg1 [enc-alg-2…]} | {**hostkey** host-alg1[host-alg2…]} | {**kex** kex-alg1[kex-alg2…]} | {**mac** mac-alg1[mac-alg2…]}

no ip ssh server algorithm {**encryption** enc-alg1 [enc-alg-2…]} | {**hostkey** host-alg1[

host-alg2…]} | {**kex** kex-alg1[kex-alg2…]} | {**mac** mac-alg1[mac-alg2…]}

Parameters

- **encryption** enc-alg1 [enc-alg-2…] (optional) — Enable one or more of the followingSSH encryption algorithms:

- aes128-ctr - AES with 128-bit key in CTR mode
- aes192-ctr - AES with 192-bit key in CTR mode
- aes256-ctr - AES with 256-bit key in CTR mode
- chacha20-poly1305 - Chacha20 with Poly1305 and 256-bit key. Compatible with chacha20-poly1305@openssh.com
- aes128-gcm - AES with 128-bit key in GCM mode. Compatible with aes128-gcm@openssh.com
- aes256-gcm - AES with 256-bit key in GCM mode. Compatible with aes256-gcm@openssh.com

- **hostkey** host-alg1[host-alg2…] (optional) — Enable one or more of the following SSH host-key public key algorithms:
  - ssh-dss - DSA public-key signature with SHA1 hash
  - ssh-rsa - RSA public-key signature with SHA1 hash
  - rsa-sha2-256 - RSA public-key with SHA2-256 hash
  - rsa-sha2-512 - RSA public-key with SHA2-512 hash

- **kex** kex-alg1[kex-alg2...] — Enable one or more of the following SSH key exchange (kex) algorithms:
  - diffie-hellman-group16-sha512 - Diffie-Hellman key exchange using SHA2-512 as HASH and 4096-bit MODP Group
  - diffie-hellman-group14-sha1 - Diffie-Hellman key exchange using SHA1 as HASH and 2048-bit MODP Group

- mac mac-alg1[mac-alg2…] (optional) — Enable one or more of the following SSH Message Authentication Code (MAC) algorithms:
  - hmac-sha1 - HMAC-SHA1 (digest length = key length = 160 bits)
  - hmac-sha2-256 - HMAC-SHA2-256 (digest length = key length = 256 bits)
  - hmac-sha2-512 - HMAC-SHA2-512 (digest length = key length = 512 bits)

Default Configuration

- Enabled Encryption algorithms: aes128-ctr, aes192-ctr, aes256-ctr, chacha20-poly1305, aes128-gcm and aes256-gcm
- Enabled host-key alogrithms: ssh-dss, ssh-rsa, rsa-sha2-256 and rsa-sha2-512
- Enabled kex algorithms: diffie-hellman-group16-sha512 and diffie-hellman-group14-sha1
- Enabled MAC algorithms: hmac-sha1, hmac-sha2-256 and hmac-sha2-512

Command Mode

Global Configuration mode

User Guidelines

Use the ip ssh server algorithm command to specify which encryption, host-key, key exchange (kex) and MAC algorithm will be advertised to the SSH client. Algorithms not specified in the command will not be advertised. The no ip ssh server algorithm specifies which algorithms to remove from the advertisement to the SSH client.

The no command will change the advertisement list only if it specifies an algorithm that is in the current advertisement list. At least one algorithm must be supported for each category. If the command attempts to remove the last algorithm supported for that category the operation will fail and an error message will be displayed.

The configuration file will include a command that specifies the algorithm that are advertised (even if no ip ssh server algorithm was used for the configuration).

The following algorithms are supported, and can be disabled only if FIPS mode is disabled:

- chacha20-poly1305 encryption
- ssh-dss host-key

In FIPS enabled mode these algorithms are not supported, and therefore do not need to be disabled.

Example

The following example enables a few of the SSH encryption algorithms on the device. This means that the other encryption algorithms will not be advertised to the SSH client:

```
switchxxxxxx(config)# ip ssh server encryption aes256-ctr aes256-gcm
```

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: 1–59999).

Default Configuration

The default TCP port number is 22.

Command Mode

Global Configuration mode

Example

The following example specifies that TCP port number 808 is used by the SSH server.

```
switchxxxxxx(config)# ip ssh port 808
```

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
```

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 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 pass the device management AAA authentication independently of 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 management access is granted only if the user is AAA authenticated by the device management. No SSH authentication method means SSH is enabled and 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
```

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-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-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
```

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-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

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-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-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-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row AAAAB3Nza
switchxxxxxx(config-keychain-key)# key-string row C1yc2
```

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
SSH session logging is disabled
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

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.

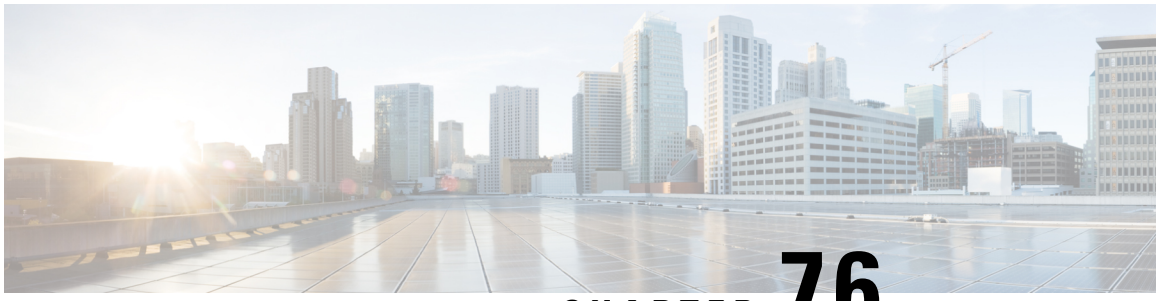
Command Mode

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
```



CHAPTER 76

IPv6 Tunnel Commands

This chapter contains the following sections:

- interface tunnel, on page 1207
- tunnel destination, on page 1208
- tunnel isatap solicitation-interval, on page 1208
- tunnel isatap robustness, on page 1209
- tunnel isatap router, on page 1210
- tunnel mode ipv6ip, on page 1211
- tunnel source, on page 1213
- show ipv6 tunnel, on page 1214

interface tunnel

To enter into the Interface Configuration (Tunnel) mode, use the **interface tunnel** command in Global Configuration mode.

Syntax

interface tunnel *number*

Parameters

- ***number***—Specifies the tunnel number.

Command Mode

Global Configuration mode

Example

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

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source auto
switchxxxxxx(config-if)# exit
```

tunnel destination

To specify the destination IPv4 address for the manual tunnel interface, use the **tunnel destination** command in Interface (Tunnel) Configuration mode. To remove the destination IPv4 address, 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

Interface (Tunnel) Configuration mode

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:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 10.0.0.1 255.255.255.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface tunnel1
switchxxxxxx(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
switchxxxxxx(config-if)# tunnel source vlan1
switchxxxxxx(config-if)# tunnel destination 192.168.30.1
switchxxxxxx(config-if)# tunnel mode ipv6ip
switchxxxxxx(config-if)# exit
```

tunnel isatap solicitation-interval

To set the time interval between unsolicited router solicitation messages, use the **tunnel isatap solicitation-interval** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

tunnel isatap solicitation-interval *seconds*

no tunnel isatap solicitation-interval

Parameters

- ***seconds***—Specifies the time interval in seconds between ISATAP router solicitation messages. (Range: 10–3600).

Default Configuration

The default time interval between ISATAP router solicitation messages is 10 seconds.

Command Mode

Global Configuration mode

User Guidelines

This command determines the interval between unsolicited router solicitation messages sent to discovery an ISATAP router.

Example

The following example sets the time interval between ISATAP router solicitation messages to 30 seconds.

```
switchxxxxxx(config)# tunnel isatap solicitation-interval 30
```

tunnel isatap robustness

To configure the number of router solicitation refresh messages that the device sends, use the **tunnel isatap robustness** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

tunnel isatap robustness *number*

no tunnel isatap robustness

Parameters

- ***number***—Specifies the number router solicitation refresh messages that the device sends. (Range: 1–20).

Default Configuration

The default number of router solicitation refresh messages that the device sends is 3.

Command Mode

Global Configuration mode

User Guidelines

The router solicitation interval (when there is an active ISATAP router) is the minimum-router-lifetime that is received from the ISATAP router, divided by (Robustness + 1).

Example

The following example sets the number of router solicitation refresh messages that the device sends to 5.

```
switchxxxxxx(config)# tunnel isatap robustness 5
```

tunnel isatap router

To configure a global string that represents a specific automatic tunnel router domain name, use the **tunnel isatap router** command in Interface (Tunnel) Configuration mode. To remove this router name and restore the default configuration, use the **no** form of this command.

Syntax

tunnel isatap router *router-name*

no tunnel isatap router

Parameters

- ***router-name***—Specifies the router's domain name.

Default Configuration

The automatic tunnel router's default domain name is ISATAP.

Command Mode

Interface (Tunnel) Configuration mode

User Guidelines

This command determines the string that the host uses for automatic tunnel router lookup in the IPv4 DNS procedure. By default, the string **ISATAP** is used for the corresponding automatic tunnel types.

Only one string can represent the automatic tunnel router name per tunnel. Using this command, therefore, overwrites the existing entry.

The empty string means that automatic lookup is not applied.

Example

The following example configures the global string ISATAP2 as the automatic tunnel router domain name.

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel isatap router ISATAP2
switchxxxxxx(config-if)# exit
```

tunnel mode ipv6ip

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

Syntax

tunnel mode ipv6ip [6to4 | isatap]

no tunnel mode ipv6ip

Parameters

- **6to4**—(Optional) Specifies IPv6 automatic tunneling mode using a 6to4 address.
- **isatap**—(Optional) Specifies IPv6 automatic tunneling mode as ISATAP to connect IPv6 nodes (hosts and routers) within IPv4 networks.

Default Configuration

IPv6 tunnel interfaces are not configured.

Command Mode

Interface (Tunnel) Configuration mode

User Guidelines

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

The IPv6 interface is automatically enabled on a tunnel when it is configured as an IPv6 tunnel by the **tunnel mode ipv6ip** command and the local IPv4 is defined by the **tunnel source** command.

When the IPv6 tunnel mode is changed the IPv6 interface on the tunnel is re-enabled that causes removing static IPv6 configuration on the tunnel (for example, global IPv6 addresses, static IPv6 routes via the tunnel, etc.).

The IPv6 interface on an IPv6 tunnel is disabled if the tunnel stops to be an IPv6 tunnel or the tunnel local IPv4 address is removed and the new IPv4 cannot be chosen.

Manually Configured Tunnels

Using this command without keywords specifies an IPv6-configured tunnel where the tunnel endpoints is determined by two manually configured unique IPv4 addresses by the **tunnel source** and **tunnel destination** commands. Only the **ipv6 address eui-64** command can be used to configured a global unicast IPv6 on a manual tunnel. Any correct global 64-bits IPv6 prefix can be configured.

The interface identifier of tunnel is 0:0:WWXX:YYZZ, where WWXX:YYZZ is the tunnel local IPv4 address (RFC 4213).

6to4 Tunnels

Using this command with the **6to4** keyword specifies automatic 6to4 tunneling where only the local tunnel endpoint is determined by manually configured unique IPv4 address.

During the 6to4 tunnel creation the switch automatically creates on the 6to4 tunnel:

- IPv6 interface
- Unicast global IPv6 address 2002:WWXX:YYZZ::WWXX:YYZZ/64, where WWXX:YYZZ is 32 bits of the local tunnel IPv4 address (RFC 3056).
- On-link route 2002::/16

A global unicast IPv6 address cannot be configured manually on a 6to4 tunnel.

The unique IPv4 address is used as the network-layer address in the 6to4 address prefix. A unicast global 64-bits 6to4 IPv6 prefix (RFC 3056) 2002:WWXX:YYZZ:SSI::/64 (SSI - 16 bits of Site Subnet Identifier.) can be used for definition unicast global 6to4 IPv6 addresses on native IPv6 the in-band interfaces on switch.

ISATAP Tunnels

Using this command with the **isatap** keyword specifies an automatic ISATAP tunnel. ISATAP tunnels enable transport of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

ISATAP IPv6 addresses can use any initial Unicast /48 prefix. The final 64 bits are an interface identifier. Of these, the leading 32 bits are the fixed pattern 0000:5EFE; the last 32 bits carry the tunnel endpoint IPv4 address.

Only the **ipv6 address eui-64** command can be used to configured a global unicast IPv6 on an ISATAP tunnel.

Example 1—The following example configures an ISATAP tunnel:

```
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip address 1.1.1.1 255.255.255.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# tunnel mode ipv6ip isatap
switchxxxxxx(config-if)# tunnel source 1.1.1.1
switchxxxxxx(config-if)# ipv6 address 3ffe:b00:c18:1::/64 eui-64
switchxxxxxx(config-if)# exit
```

Example 2—The following example 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:

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source vlan 1
switchxxxxxx(config-if)# tunnel destination 192.168.30.1
switchxxxxxx(config-if)# tunnel mode ipv6ip
switchxxxxxx(config-if)# exit
```

Example 3—The following example configures a 6to4 tunnel:

```
switchxxxxxx(config)# interface vlan 100
switchxxxxxx(config-if)# ip address 192.168.99.1 255.255.255.0
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source vlan 100
switchxxxxxx(config-if)# tunnel mode ipv6ip 6to4
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 101
switchxxxxxx(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
switchxxxxxx(config-if)# exit
switchxxxxxx(config)# interface vlan 102
```

```
switchxxxxxx(config-if)# ipv6 address 2002:c0a8:6301:2::/64 eui-64
switchxxxxxx(config-if)# exit
```

tunnel source

To set the local (source) IPv4 address of a tunnel interface, use the **tunnel source** command in Interface (Tunnel) Configuration mode. To delete the tunnel local address, use the **no** form of the command.

Syntax

tunnel source {**auto** | *ipv4-address* | *interface-id*}

no tunnel source

Parameters

- **auto**—The system minimum IPv4 address is used as the local IPv4 address (IPv4 address of the local tunnel endpoint).
- ***ip4-address***—Specifies the IPv4 address to use as the local IPv4 address (IPv4 address of the local tunnel endpoint).
- ***interface-id***—Interface which the minimum IPv4 address is used as the local IPv4 address (IPv4 address of the local tunnel endpoint).

Default

No source address is defined.

Command Mode

Interface (Tunnel) Configuration mode

User Guidelines

If the **auto** or *interface-id* option is configured once time chosen IPv4 is used as the tunnel local IPv4 address until it is defined. A new IPv4 interface is only chosen in the following cases:

- After reboot.
- The used IPv4 is removed from the switch configuration.
- The tunnel mode is changed.

When the tunnel local IPv4 address is changed the IPv6 interface on the tunnel is re-enabled that causes removing static IPv6 configuration on the tunnel (for example, global IPv6 addresses, static IPv6 routes via the tunnel, etc.).

If the **auto** option is configured then the IP addresses defined on OOB do not take part in the choosing of the minimal IPv4 address.

If the *ip4-address* option is configured then the IPv4 addresses defined on OOB cannot be configured.

If the *interface-id* option is configured then OOB cannot be configured.

Example

```
switchxxxxxx(config)# interface tunnel 1
switchxxxxxx(config-if)# tunnel source 120.12.3.4
switchxxxxxx(config-if)# exit
```

show ipv6 tunnel

To display information on IPv6 tunnels, use the **show ipv6 tunnel** command in User EXEC mode.

Syntax

show ipv6 tunnel [**all**]

Parameters

- **all**—(Optional) 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

User EXEC mode

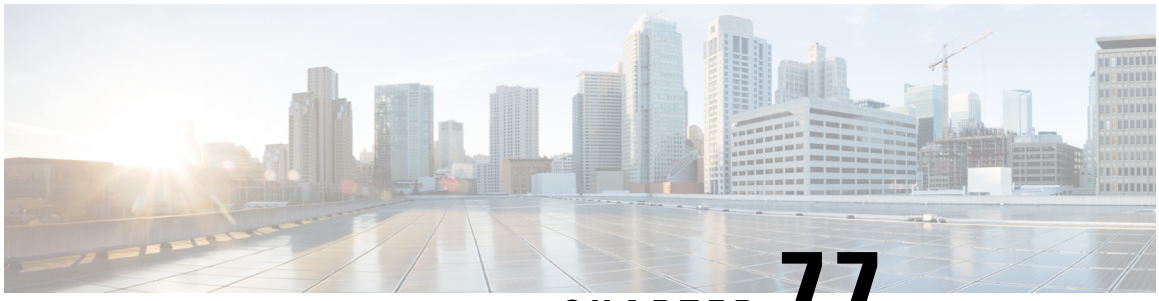
Example 1. The following example displays information on the ISATAP tunnel, when the all keyword is not configured:

```
switchxxxxxx# show ipv6 tunnel
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                      : ISATAP
  Tunnel status                    : UP
  Tunnel Local address type        : auto
  Tunnel Local Ipv4 address        : 192.1.3.4
  Router DNS name                  : ISATAP
  Router IPv4 addresses
    1.1.1.1          Detected
    100.1.1.1        Detected
    14.1.100.1       Not Detected
  Router Solicitation interval     : 10 seconds
Robustness : 2

Tunnel 3
  Tunnel type                      : 6to4
  Tunnel status                    : UP
  Tunnel Local address type        : auto
  Tunnel Local Ipv4 address        : 192.1.3.4
```

Example 2. The following example displays information when the **all** keyword is configured:

```
switchxxxxxx# show ipv6 tunnel all
Tunnel 1
  Tunnel type                      : Manual
  Tunnel status                    : UP
  Tunnel Local address type        : VLAN 100
```

```
  Tunnel Local Ipv4 address        : 192.1.3.4
  Manual parameters
    Tunnel Remote Ipv4 address     : 192.3.4.5
  ISATAP Parameters
    Router DNS name                : ISATAP
    Router Solicitation interval   : 10 seconds
 Robustness : 2

Tunnel 2
  Tunnel type                      : Manual
  Tunnel status                    : DOWN
  Tunnel Local address type        : auto
  Manual parameters
    Tunnel Remote Ipv4 address     : 0.0.0.0
  ISATAP Parameters
    Tunnel Local Ipv4 address      : 0.0.0.0
    Router DNS name                : ISATAP
    Router Solicitation interval   : 10 seconds
Robustness : 2

Tunnel 3
  Tunnel type                      : ISATAP
  Tunnel status                    : UP
  Tunnel Local address type        : auto
  Manual parameters
    Tunnel Remote Ipv4 address     : 0.0.0.0
  ISATAP Parameters
    Tunnel Local Ipv4 address      : 192.1.3.4
    Router DNS name                : ISATAP
    Router IPv4 addresses
      1.1.1.1          Detected
      100.1.1.1        Detected
      14.1.100.1       Not Detected
    Router Solicitation interval   : 10 seconds
 Robustness : 2
```



CHAPTER 77

UDLD Commands

This chapter contains the following sections:

- show udld, on page 1217
- udld, on page 1220
- udld message time, on page 1221
- udld port, on page 1221

show udld

To display the administrative and operational Unidirectional Link Detection Protocol (UDLD) status, use the **show udld** command in Privileged EXEC mode.

Syntax

show udld [*interface-id*] [**neighbors**]

Parameters

- ***interface-id***—Interface identifier of an Ethernet port.
- **neighbors**—Displays neighbor information only.

Command Mode

Privileged EXEC mode

User Guidelines

If you do not enter an interface ID value, the administrative and operational UDLD status for all interfaces on which UDLD is enabled are displayed.

Example 1—This example shows how to display the UDLD state for all interfaces. Most of the fields shown in the display are self-explanatory. Those that are not self-explanatory are defined below.

```
switchxxxxxx# show udld
Global UDLD mode: normal
Message Time: 15 sec(default)
```

```
Interface gi1/0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
    Neighbor Device ID: 1234544893
      Neighbor MAC: 00:00:01:22:33:ff
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 17 sec
Interface gi1/0/2
  Port UDLD mode: normal (default)
  Port Current state: Undetermined
  Number of detected neighbors: 1
    Neighbor Device ID: 1234567753
      Neighbor MAC: 00:00:01:22:33:fe
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 11 sec
Interface gi1/0/3
  Port UDLD mode: disabled
Interface gi1/0/4
  Port UDLD mode: normal (default)
  Port Current state: shutdown
Field Descriptions:
```

- **Global UDLD mode**—The global UDLD mode (normal or aggressive) configured by the **udld** command.
- **Message Time**—The message time configured by the **udld message time** command.
- **Port UDLD mode**—The interface UDLD mode (normal or aggressive).
- **Port Current state**—The UDLD operational state: interface UDLD mode (normal or aggressive).
  - **Disabled**—UDLD is disabled on the port by the **udld port disable** command.
  - **Shutdown**—UDLD is enabled on the port and the port operational state is DOWN.
  - **Detection**—UDLD is detecting the link state.
  - **Bidirectional**—The link is bidirectional.
  - **Undetermined**—The link state is undetermined - no UDLD message has been received on the port.
- **Neighbor Device ID**—The device ID of the neighbor.
- **Neighbor MAC**—The MAC address of the neighbor.
- **Neighbor Device Name**—The Device name of the neighbor.

- **Neighbor Port ID**—The device port ID of the neighbor on which the recent UDLD message was sent.
- **Neighbor Message Time**—The message time of the neighbor.
- **Neighbor Current State**—The current state of the neighbor:

  Bidirectional—The UDLD messages received from the neighbor contain the Device ID and Port ID of the switch in the Echo TLV.

  Undetermined—The UDLD messages received from the neighbor do not contain the Device ID and Port ID of the switch in the Echo TLV.
- **Neighbor Expiration Time**—Left time in seconds until the current neighbor state expires.

Example 2—This example shows how to display the UDLD state for one given interface:

```
switchxxxxxx# show udld gi1/0/1
Global UDLD mode: normal
Message Time: 15 sec(default)
Interface gi1/0/1
  Port UDLD mode: aggressive
  Port Current state: Bidirectional
  Number of detected neighbors: 1
  Port Neighbor Table
    Neighbor Device ID: 1234567893
      Neighbor MAC: 00:00:01:22:33:dd
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 20 sec
      Neighbor Current State: Bidirectional
      Neighbor Expiration Time: 7 sec
    Neighbor Device ID: 1234544893
      Neighbor MAC: 00:00:01:22:33:ff
      Neighbor Device name: switch A
      Neighbor Port ID: gi1/2/1
      Neighbor Message Time: 15 sec
      Neighbor Current State: Undetermined
      Neighbor Expiration Time: 17 sec
```

Example 3—This example shows how to display neighbor information only:

```
switchxxxxxx# show udld neighbors
Port      Device ID     Port-ID   Device Name     Message    Neighbor     Expiration
                                                Time(sec) State       Time (sec)
-------- -------------- --------- --------------- --------- ----------   ---------
gi1/0/1  1234567893     gi1/0/1   SAL0734K5R2        15      Bidirect          11
gi1/0/2  3456750193     gi1/0/2   SAL0734K5R3        20      Undetermined      5
```

Example 4—This example shows how to display neighbor information only for a single interface:

```
switchxxxxxx# show udld gi1/0/1 neighbors
Port      Device ID     Port-ID   Device Name     Message    Neighbor     Expiration
                                                Time(sec) State       Time (sec)
-------- -------------- --------- --------------- --------- ----------   ---------
gi1/0/1  1234567893    gi1/0/1   SAL0734K5R2        15      Bidirect          11
```

udld

Use the **udld** command in Global Configuration mode to globally enable the UniDirectional Link Detection (UDLD) protocol. To disable UDLD, use the **no** form of this command.

Syntax

udld aggressive | **normal**

no udld

Parameters

- **aggressive**—Enables UDLD in aggressive mode by default on all fiber interfaces.
- **normal**—Enables UDLD in normal mode by default on all fiber interfaces.

Default Configuration

UDLD is disabled on all fiber interfaces.

Command Mode

Global Configuration mode

User Guidelines

This command affects fiber interfaces only. Use the **udld port** command in Interface Configuration mode to enable UDLD on other interface types.

Use the **no** form of this command to disable UDLD on all fiber ports.

The device supports the UDLD protocol specified by RFC 5171.

UDLD supports two modes of operation: normal and aggressive. In the aggressive mode the device shuts down a port if it cannot explicitly detect that the link is bidirectional. In the normal mode the device shuts down an interface if it explicitly detect that the link is unidirectional. A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

You can use the following commands to reset an interface shut down by UDLD:

- The **errdisable recover reset** command with the **interface** *interface-id* parameter to reset a given interface.
- The **errdisable recover reset** command with the **udld** parameter to reset all interfaces shut down by UDLD.
- The **errdisable recover cause** with the **udld** parameter to automatically recover from the UDLD error-disabled state.

Example

This example shows how to enable UDLD on all fiber interfaces:

```
switchxxxxxx(config)# udld normal
```

udld message time

Use the **udld message time** command in Global Configuration mode to configure a global value of the interval between two sent probe messages. To return to the default value, use the **no** form of this command.

Syntax

udld message time *seconds*

no udld message time

Parameters

seconds—Interval between two sent probe messages. The valid values are from 1 to 90 seconds.

Default Configuration

15 seconds.

Command Mode

Global Configuration mode

User Guidelines

Use this command to change the default value of the message interval - the interval between two sequential sent probe messages.

Example

This example shows how to globally set the interval to 40sec:

```
switchxxxxxx(config)# udld message time 40
```

udld port

To enable the UDLD protocol on an Ethernet port, use the **udld port** command in Interface Configuration mode. To return to the default, use the **no** form of this command.

Syntax

udld port [**aggressive** | **normal** | **disable**]

no udld port

Parameters

- **aggressive**—Enables UDLD in aggressive mode on this interface.
- **normal**—Enables UDLD in normal mode on this interface. The normal keyword is applied if no keyword is specified.

- **disable**—Disables UDLD on this interface.

Default Configuration

The defaults are as follows:

- Fiber interfaces are in the state configured by the **udld** command.
- Non-fiber interfaces are in the Disable state.

Command Mode

Interface (Ethernet) Configuration mode

User Guidelines

Use this command on fiber ports to override the setting of the global **udld** command.

If the port changes from fiber to non-fiber or vice versa, all configurations are maintained because the platform software detects a change of module or a Gigabit Interface Converter (GBIC) change.

Example 1—This example shows how to enable UDLD in normal mode on an Ethernet port regardless of the current global **udld** setting:

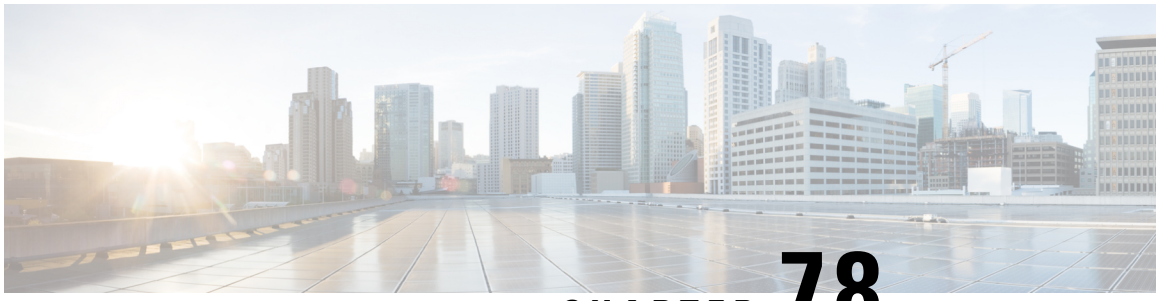
```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# udld port normal
switchxxxxxx(config-if)# exit
```

Example 2—This example shows how to return to the default configuration:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no udld port
switchxxxxxx(config-if)# exit
```

Example 3—This example shows how to disable UDLD on an Ethernet port regardless of the current global **udld** setting:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# udld port disable
switchxxxxxx(config-if)# exit
```



CHAPTER 78

User Interface Commands

This chapter contains the following sections:

- banner exec, on page 1223
- banner login, on page 1225
- configure, on page 1226
- disable, on page 1226
- do, on page 1227
- enable, on page 1228
- end, on page 1228
- exit (Configuration), on page 1229
- exit (EXEC), on page 1230
- help, on page 1230
- history, on page 1231
- history size, on page 1232
- login, on page 1232
- terminal datadump, on page 1233
- terminal history, on page 1234
- terminal history size, on page 1234
- terminal prompt, on page 1235
- terminal width, on page 1236
- show banner, on page 1236
- show history, on page 1237
- show privilege, on page 1238

banner exec

To specify and enable a message to be displayed after a successful logon, use the **banner exec** Global Configuration mode command. This banner is applied automatically on all the user interfaces: console, Telnet and SSH and also on the WEB GUI. To delete the existing EXEC banner, use the **no** form of this command.

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 1000 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.
$(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.
```

banner login

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

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 1000 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.

Token	Information displayed in the banner
$(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
```

configure

To enter the Global Configuration mode, use the **configure** Privileged EXEC mode command.

Syntax

configure [*terminal*]

Parameters

terminal—(Optional) 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)#
```

disable

To leave the Privileged EXEC mode and return to the User EXEC mode, use the **disable** Privileged EXEC mode command.

Syntax

disable [*privilege-level*]

Parameters

privilege-level—(Optional) Reduces the privilege level to the specified privileged level. If privilege level is left blank, the level is reduce to the minimal privilege level.

Default Configuration

The default privilege level is 15.

Command Mode

Privileged EXEC mode

Example

The following example returns the user to user level 1.

```
switchxxxxxx# disable 1
switchxxxxxx#
```

do

To execute an EXEC-level command from Global Configuration mode or any configuration submode, use the **do** command.

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.

```
switchxxxxxx(config)# do show vlan
```

Vlan	Name	Ports	Type	Authorization
----	----	-----	----	----------
1	1	gi1/0/1-4,Po1,Po2	other	Required
2	2	gi1/0/1	dynamicGvrp	Required

10	v0010	gi1/0/1	permanent	Not Required
11	V0011	gi1/0/1,gi1/0/3	permanent	Required
20	20	gi1/0/1	permanent	Required
30	30	gi1/0/1,gi1/0/3	permanent	Required
31	31	gi1/0/1	permanent	Required
91	91	gi1/0/1,gi1/0/4	permanent	Required
4093	guest-vlan	gi1/0/1,gi1/0/3	permanent	Guest

```
switchxxxxxx(config)#
```

enable

To enter the Privileged EXEC mode, use the **enable** User EXEC mode command.

Syntax

enable [*privilege-level*]

Parameters

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

Default Configuration

The default privilege level is 15.

Command Mode

User EXEC mode

Example

The following example enters privilege level 7.

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

The following example enters privilege level 15.

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

end

To end the current configuration session and return to the Privileged EXEC mode, use the **end** command.

Syntax

end

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Example

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

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

exit (Configuration)

To exit any mode and bring the user to the next higher mode in the CLI mode hierarchy, use the **exit** command.

Syntax

exit

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

Examples

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

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

exit (EXEC)

To close an active terminal session by logging off the device, use the **exit** User EXEC mode command.

Syntax

exit

Parameters

This command has no arguments or keywords

Command Mode

User EXEC mode

Example

The following example closes an active terminal session.

```
switchxxxxxx#  exit
```

help

To display a brief description of the Help system, use the **help** command.

Syntax

help

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

All configuration modes

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?').
```

history

To enable saving commands that have been entered, use the **history** Line Configuration Mode command. To disable the command, use the **no** form of this command.

Syntax

history

no history

Parameters

This command has no arguments or keywords

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, on page 1234 User EXEC mode command to enable or disable this command for the current terminal session.

  Use the history size, on page 1232 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
```

history size

To change the maximum number of user commands that are saved in the history buffer for a particular line, use the **history size** Line Configuration Mode command. To reset the command history buffer size to the default value, use the **no** form of this command.

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** User 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
```

login

To enable changing the user that is logged in, use the **login** User EXEC mode command. When this command is logged in, the user is prompted for a username/password.

Syntax

login

Parameters

This command has no arguments or keywords

Command Mode

User 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#
```

terminal datadump

To enable dumping all the output of a show command without prompting, use the **terminal datadump** User EXEC mode command. To disable dumping, use the **no** form of this command.

Syntax

terminal datadump

terminal no datadump

Parameters

This command has no arguments or keywords

Default Configuration

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

Command Mode

User 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
```

terminal history

To enable the command history function for the current terminal session, meaning that it will not be stored in the Running Configuration file, use the **terminal history** User EXEC mode command. To disable the command, use the **no** form of this command.

Syntax

terminal history

terminal no history

Parameters

This command has no arguments or keywords

Default Configuration

The default configuration for all terminal sessions is defined by the history, on page 1231 Line Configuration Mode command.

Command Mode

User EXEC mode

User Guidelines

The command enables the command history for the current session. The default is determined by the history, on page 1231 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
```

terminal history size

To change the command history buffer size for the current terminal session, meaning it will not be stored in the Running Configuration file, use the **terminal history size** User EXEC mode command. , 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: 10–206)

Default Configuration

The default configuration for all terminal sessions is defined by the history size, on page 1232 Line Configuration Mode command.

Command Mode

User EXEC mode

User Guidelines

The **terminal history size** EXEC command changes the command history buffer size for the current terminal session. Use the history, on page 1231 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
```

terminal prompt

To enable the terminal prompts, use the **terminal prompt** User EXEC mode command. To disable the terminal prompts, use **terminal no prompt** command.

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

Syntax

terminal prompt

terminal no prompt

Parameters

This command has no arguments or keywords

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
```

terminal width

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

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
```

show banner

To display the banners that have been defined, use the **show banner** commands in User EXEC mode.

Syntax

show banner login

show banner exec

Parameters

This command has no arguments or keywords

Command Mode

User EXEC mode

Examples

```
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
```

show history

To list the commands entered in the current session, use the **show history** User EXEC mode command.

Syntax

show history

Parameters

This command has no arguments or keywords

Command Mode

User 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)
```

show privilege

To display the current privilege level, use the **show privilege** User EXEC mode command.

Syntax

show privilege

Parameters

This command has no arguments or keywords

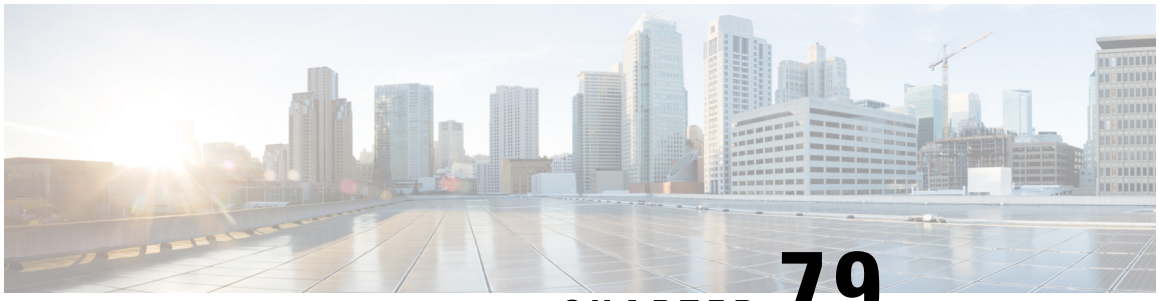
Command Mode

User EXEC mode

Example

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

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



CHAPTER 79

VLAN Commands

This chapter contains the following sections:

- vlan database, on page 1240
- vlan , on page 1241
- show vlan, on page 1241
- interface vlan, on page 1242
- interface range vlan, on page 1243
- name, on page 1243
- switchport protected-port, on page 1244
- show interfaces protected-ports, on page 1245
- switchport, on page 1245
- switchport mode, on page 1246
- switchport access vlan , on page 1248
- switchport trunk native vlan , on page 1249
- switchport trunk allowed vlan , on page 1250
- switchport general allowed vlan , on page 1251
- switchport general pvid, on page 1252
- switchport general ingress-filtering disable, on page 1253
- switchport general acceptable-frame-type, on page 1253
- switchport general forbidden vlan , on page 1254
- switchport customer vlan, on page 1255
- ethtype, on page 1255
- switchport nni ethtype, on page 1256
- switchport vlan-mapping tunnel, on page 1257
- switchport vlan-mapping tunnel l2protocol vlan, on page 1259
- switchport vlan-mapping tunnel l2protocol cos, on page 1260
- switchport vlan-mapping tunnel l2protocol cos interface, on page 1260
- switchport vlan-mapping tunnel l2protocol drop-threshold, on page 1261
- switchport vlan-mapping tunnel l2protocol forward, on page 1262
- switchport vlan-mapping one-to-one, on page 1264
- map protocol protocols-group, on page 1265
- switchport general map protocols-group vlan, on page 1266
- show vlan protocols-groups, on page 1267
- map mac macs-group, on page 1267

- switchport general map macs-group vlan, on page 1268
- show vlan macs-groups, on page 1269
- map subnet subnets-group, on page 1270
- switchport general map subnets-group vlan, on page 1270
- show vlan subnets-groups, on page 1271
- show interfaces switchport, on page 1272
- private-vlan, on page 1273
- private-vlan association, on page 1274
- switchport private-vlan mapping, on page 1275
- switchport private-vlan host-association, on page 1276
- show vlan private-vlan, on page 1277
- switchport access multicast-tv vlan, on page 1277
- switchport customer multicast-tv vlan, on page 1278
- show vlan multicast-tv, on page 1279
- vlan prohibit-internal-usage, on page 1279
- show vlan internal usage , on page 1281

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

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
```

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* | {*vlan-id* [**name** *vlan-name*]} [**media ethernet**] [**state active**]

no vlan *vlan-range*

Parameters

- ***vlan-range***—Specifies a list of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs (range: 2-4094).
- ***vlan-id***—Specifies a VLAN ID. (range: 2-4094).
- ***vlan-name***—Specifies the VLAN name. (range: 1–32 characters).
- **media**—Specifies the media type of the VLAN. Valid values are **ethernet**.
- **state**—Specifies whether the state of the VLAN. Valid values are **active**.

Default Configuration

VLAN 1 exists by default.

Command Mode

Global Configuration mode

VLAN Database Configuration mode

User Guidelines

If the VLAN does not exist, it is created. If the VLAN cannot be created then the command is finished with error and the current context is not changed.

Example

The following example creates a few VLANs. VLAN 1972 is assigned the name Marketing.

```
switchxxxxxx(config)# vlan database
switchxxxxxx(config-vlan)# vlan 19-23
switchxxxxxx(config-vlan)# vlan 100
switchxxxxxx(config-vlan)# vlan 1972 name Marketing
switchxxxxxx(config-vlan)# exit
```

show vlan

Use the **show vlan** Privileged EXEC mode command to display the following VLAN information.

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

Example 1—The following example displays information for all VLANs:

```
switchxxxxxx# show vlanCreated by: S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN
```

VLAN	Name	Tagged Ports	UnTagged Ports	Created by
-----	----------	----------	----------	----------
1	Default		gi1/0/1	S
10	Marketing	gi1/0/2	gi1/0/2	S
91	11	gi1/0/2-4	gi1/0/2	SGR
92	11	gi1/0/3-4		G
93	11	gi1/0/3-4		GR

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.

Syntax

interface vlan *vlan-id*

Parameters

- ***vlan-id***—Specifies the VLAN to be configured.

Command Mode

Global Configuration mode

User Guidelines

If the VLAN does not exist, the VLAN is created. If the VLAN cannot be created, this command is finished with an error and the current context is not changed.

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
```

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-range***—Specifies a list of VLANs. Separate nonconsecutive VLANs with a comma and no spaces. Use a hyphen to designate a range of VLANs.

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
```

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 (VLAN) Configuration mode

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
```

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

Default Configuration

Unprotected

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

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.

Example

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport protected-port
```

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

User EXEC mode

Example

```
switchxxxxxx# show interfaces protected-ports
```

Interface	State
gi1/0/1	Protected
gi1/0/2	Protected
gi1/0/3	Unprotected
gi1/0/4	Unprotected

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

Default Configuration

Layer 2 mode

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **no switchport** command to set the interface as a Layer 3 interface.

An interface cannot be set as a Layer 3 interface if 802x.1 is enabled on the interface and one of the following conditions is true:

- The host mode differs from multi-host.
- MAC-Based or WEB-Based authentication is enabled.
- Radius VLAN assignment is enabled.

Examples

Example 1 - The following example puts the port gi1/0/1 into Layer 2 mode.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport
```

Example 2 - The following example puts the port gi1/0/1 into Layer 3 mode.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# no switchport
```

switchport mode

Use the **switchport mode** Interface Configuration mode command to configure the VLAN membership mode. Use the **no** form of this command to restore the default configuration.

Syntax

switchport mode access | **trunk** | **general** | **private-vlan** {**promiscuous** | **host**} | **customer** | **vlan-mapping** {**tunnel** | **one-to-one** }

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 an edge port connected to customer equipment. Traffic received from this port will be tunneled with the additional 802.1q VLAN tag (Q-in-Q VLAN tunneling).
- **private-vlan promiscuous**—Private-VLAN promiscuous port.

- **private-vlan host**—Private-VLAN host port.
- **vlan-mapping tunnel**—VLAN Mapping tunel edge port.
- **vlan-mapping one-to-one**—VLAN Mapping one-to-one edge port.

Default Configuration

Access mode.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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.

Use the **switchport mode vlan-mapping** {**tunnel** | **one-to-one**} command to configure a VLAN mapping mode of an edge interface of a Provider Edge switch. The edge interface is an interface where a Customer network is connected to the Provider Edge switch. The network which the switch belongs to is a Provider network. These networks (Customer ones and Provider one) can use the same VLAN-IDs and the edge interface must perform vlan mapping between Customer VLANs (C-VLANs) and Provider VLANs (S-VLANs).

On an edge interface C-VLANs are mapped to S-VLANs and the original C-VLAN tags are kept as part of payload. When a frame is sent on non-edge tagged interface, it is encapsulated with another layer of S-VLAN tag to which the original C-VLAN-ID is mapped. Therefore, transmitted on non-edge interfaces frames are double-tagged, with the outer S-VLAN tag and inner C-VLAN tag. When a frame is sent on an edge interface the S-VLAN tag is stripped.

On an edge interface C-VLANs are mapped to the S-VLANs and the original C-VLAN-ID in input frame is replaced by the S-VLAN ID to which it is mapped. Untagged frames are dropped. Symmetrical translating back to the edge interface.

The following features cannot be enabled if vlan-mapping is allowed:

- IPv4 routing
- IPv6 routing
- Auto Smart Port
- Voice VLAN

The **switchport vlan-mapping** commands cannot add a port to a S-VLAN.

IPv4 and IPv6 interfaces cannot be defined on VLANs containing edge interfaces.

The following Layer 2 features are not supported into VLANs containing edge interfaces:

- IGMP Snooping
- MLD Snooping
- DHCP Snooping

- IPv6 First Hop Security

The following protocols cannot be enabled on edge interfaces:

- STP
- GVRP

The following features are not supported on edge interfaces:

- Radius VLAN assignment
- 802.1x Guest VLAN

Egress ACLs are not supported on one-to-one VLAN mapping edge ports.

A destination port with the **network** keyword or reflector port cannot be configured on an edge port.

Note. All the limitations for edge ports specified above are checked by the **switchport vlan-mapping** commands and by the commands configuring these features.

By default the switch does not forward frames received on edge ports with the following destination MAC addresses:

- 01:80:C2:00:00:00-01:80:C2:00:00:FF
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
- 01:00:0C:CD:CD:D0

Note. The following protocols using these MAC addresses can be enabled on edge ports:

- LACP - 01:80:C2:00:00:02
- LLDP - 01:80:C2:00:00:0E
- UDLD - 01:00:0C:CC:CC:CC
- CDP - 01:00:0C:CC:CC:CC

Examples

Example 1 - The following example configures gi1/0/1 as an access port (untagged layer 2) VLAN port.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

Example 2 - The following example puts the port gi1/0/2 into private-vlan host mode.

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport mode private-vlan host
```

switchport access vlan

A port in access mode can be an untagged member of at most a single VLAN. The **switchport access vlan** Interface Configuration command reassigns an interface to a different VLAN than it currently belongs or assigns it to **none**, in which case it is not a member of any VLAN.

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

Syntax

switchport access vlan {*vlan-id* | **none**}

no switchport access vlan

Parameters

- ***vlan-id***—Specifies the VLAN to which the port is configured.
- **none**—Specifies that the access port cannot belong to any VLAN.

Default Configuration

The interface belongs to the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port is assigned to a different VLAN, it is automatically removed from its previous VLAN and added it to the new VLAN. If the port is assigned to **none**, it is removed from the previous VLAN and not assigned to any other VLAN.

Example

The following example assigns access port gi1/0/1 to VLAN 2 (and removes it from its previous VLAN).

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport mode access
switchxxxxxx(config-if)# switchport access vlan 2
```

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 mode command to define the native VLAN for a trunk interface. Use the **no** form of this command to restore the default native VLAN.

Syntax

switchport trunk native vlan {*vlan-id* | **none**}

no switchport trunk native vlan

Parameters

- ***vlan-id***—Specifies the native VLAN ID.
- **none**—Specifies the access port cannot belong to any VLAN.

Default Configuration

The default native VLAN is the Default VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

A value of the interface PVID is set to this VLAN ID.When the interface belongs to the Native VLAN it is set as VLAN untagged egress interface.

The configuration is applied only when the port mode is trunk.

Examples

The following example defines VLAN 2 as native VLAN for port gi1/0/1:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport trunk native vlan 2
switchxxxxxx(config-if)# exit
```

switchport trunk allowed vlan

A trunk interface is an untagged member of a single VLAN, and, in addition, it may be an tagged member of one or more VLANs. Use the **switchport trunk allowed vlan** Interface Configuration mode command to add/remove VLAN(s) to/from a trunk port. Use the no form of the command to return to the default.

Syntax

switchport trunk allowed vlan {**all** | **none** | *vlan-list* | **add** vlan-list | **remove** vlan-list | **except** vlan-list}

no switchport trunk allowed vlan

Parameters

- **all**—Specifies all VLANs from 1 to 4094. At any time, the port belongs to all VLANs existing at the time. (range: 1–4094).
- **none**—Specifies an empty VLAN list The port does not belong to any VLAN.
- ***vlan-list***— Specifies the list of VLAN IDs the interface is member of. The VLAN(s) specified in this command are the only VLAN(s) the port will be member of (all previous settings related to trunk VLAN membership are discarded). Use a hyphen to designate a range of IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces (range: 1-4094).
- **add** vlan-list—List of VLAN IDs to add to the port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **remove** vlan-list—List of VLAN IDs to remove from a port. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **except** vlan-list—List of VLAN IDs including all VLANs from range 1-4094 except VLANs belonging to *vlan-list*.

Default Configuration

By default, trunk ports belongs to all created VLANs.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **switchport trunk allowed vlan** command to specify which VLANs the port belongs to when its mode is configured as trunk.

Non-existed VLANs can be configured. When a non-existed VLAN is created the port will add to it automatically.

Forbidden VLANs can be configured.

Example

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

```
switchxxxxxx(config)# interface range gi1/0/1-3
switchxxxxxx(config-if)# switchport mode trunk
switchxxxxxx(config-if)# switchport trunk allowed vlan add 2-3,100
switchxxxxxx(config-if)
```

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**]

switchport general allowed vlan remove vlan-list

no switchport general allowed vlan

Parameters

- **add** vlan-list—List of VLAN IDs to add. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. (range: 1–4094)
- **remove** vlan-list—List of VLAN IDs to remove. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.
- **tagged**—Specify that packets are transmitted tagged for the configured VLANs
- **untagged**—Specify that packets are transmitted untagged for the configured VLANs (this is the default)

Default Configuration

The port is not a member of any VLAN.

Command Mode

Interface (Ethernet, Port Channel) Configuration 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. 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 in case if there are more VLANs in the vlan-list.

A non-existed VLAN cannot be configured. When a VLAN is removed it is deleted from the vlan-list.

The configuration is applied only when the port mode is general.

Example

The example adds gi1/0/1 and to VLAN 2 and 3. Packets are tagged on the egress:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport general allowed vlan add 2-3 tagged
```

switchport general pvid

Use the **switchport general pvid** Interface Configuration 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

- ***vlan-id***—Specifies the Port VLAN ID (PVID).

Default Configuration

The PVID is the Default VLAN PVID.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Examples

Example 1 - The following example sets the gi1/0/2 PVID to 234.

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport general pvid 234
```

Example 2 - The following example performs the following:

- Adds VLANs 2&3 as tagged, and VLAN 100 as untagged to gi1/0/4

- Defines VID 100 as the PVID

```
switchxxxxxx(config)# interface gi1/0/4
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)# exit
```

switchport general ingress-filtering disable

Use the **switchport general ingress-filtering disable** Interface Configuration 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

Default Configuration

Ingress filtering is enabled.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

Example

The following example disables port ingress filtering on gi1/0/1.

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general ingress-filtering disable
```

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 (Ethernet, Port Channel) Configuration mode

Example

The following example configures port gi1/0/3 to be in general mode and to discard untagged frames at ingress.

```
switchxxxxxx(config)# interface gi1/0/3
switchxxxxxx(config-if)# switchport mode general
switchxxxxxx(config-if)# switchport general acceptable-frame-type tagged-only
```

switchport general forbidden vlan

Use the **switchport general forbidden vlan** Interface Configuration mode command to forbid adding/removing specific VLANs to/from a port. Use the **no** form of this command to restore the default configuration.

Syntax

switchport general forbidden vlan {**add** *vlan-list* | **remove** vlan-list}

no switchport general forbidden vlan

Parameters

- **add** *vlan-list*—Specifies a list of VLAN IDs to add to interface. 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 interface. 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 (Ethernet, Port Channel) Configuration mode

User Guidelines

The forbidden VLAN cannot be one that does not exist on the system, or one that is already defined on the port.

Example

The following example define s gi1/0/4 as a forbidden membership in VLANs 5-7:

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport general forbidden vlan add 5-7
switchxxxxxx(config-if)# exit
```

switchport customer vlan

Use the **switchport customer vlan** Interface Configuration mode command to set the port's VLAN when the interface is in customer mode (set by the **switchport mode** command). Use the **no** form of this command to restore the default configuration.

Syntax

switchport customer vlan *vlan-id*

no switchport customer vlan

Parameters

- ***vlan-id***—Specifies the customer VLAN.

Default Configuration

No VLAN is configured as customer.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

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.

Example

The following example defines gi1/0/4 as a member of customer VLAN 5.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport mode customer
switchxxxxxx(config-if)# switchport customer vlan 5
```

ethtype

To define globally the Ethernet type used into S-VLAN tag, use the **ethtype** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

ethtype dot1q | **dot1ad** | **9100** | **9200**

no ethtype

Parameters

- **dot1q**—A value of 0x8100 (802.1q VLAN tag) is used as Ethernet tag in VLAN tag.
- **dot1ad**—A value of 0x88a8 (802.1ad VLAN tag) is used as Ethernet tag in VLAN tag.
- **9100**—A value of 0x9100 is used as Ethernet tag in VLAN tag.
- **9200**—A value of 0x9200 is used as Ethernet tag in VLAN tag.

Default Configuration

dot1q

Command Mode

Global Configuration mode

User Guidelines

Use the **ethtype** command, to define globally the Ethernet type used into S-VLAN tag. The configuration is applied to all NNI interfaces. All non-edge interfaces are considered as NNI interfaces. The edge interface is an interface having one of the following modes:

- customer
- vlan-mapping tunnel
- vlan-mapping one-to-one

Use the **no ethtype** command to restore the default configuration.

Example

This example sets the Ethernet type into the VLAN tag to dot1ad (0x88a8):

```
switchxxxxxx(config)# ethtype dot1ad
```

switchport nni ethtype

To define the Ethernet type used into S-VLAN tag on a NNI interface, use the **switchport nni ethtype** command in Interface (Ethernet, Port Channel) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport nni ethtype dot1q | **dot1ad** | **9100** | **9200**

no switchport nni ethtype

Parameters

- **dot1q**—A value of 0x8100 (802.1q VLAN tag) is used as Ethernet tag in VLAN tag.

- **dot1ad**—A value of 0x88a8 (802.1ad VLAN tag) is used as Ethernet tag in VLAN tag.
- **9100**—A value of 0x9100 is used as Ethernet tag in VLAN tag.
- **9200**—A value of 0x9200 is used as Ethernet tag in VLAN tag.

Default Configuration

Configured by the **ethtype** command.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **switchport nni ethtype** command, to define the Ethernet type used into S-VLAN tag on a NNI interface. All non-edge interfaces are considered as NNI interfaces. The edge interface is an interface having one of the following modes:

- customer
- vlan-mapping tunnel
- vlan-mapping one-to-one

Use the **no switchport nni ethtype** command to restore the default configuration.

Example

This example sets the Ethernet type into the VLAN tag to dot1ad (0x88a8):

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport nni ethtype dot1ad
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel

To configure selective tunneling on an edge interface, use the **switchport vlan-mapping tunnel** command in Interface (Ethernet, Port Channel) Configuration mode. To delete the configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping tunnel {*vlan-list* | **default**} {*outer-vlan-id* | **drop**}

no switchport vlan-mapping tunnel [*vlan-list* | **default**]

Parameters

- ***vlan-list***—Specifies the Customer VLANs (C-VLANs) for selective tunneling. The VLAN IDs in the list are separated by a comma or a series of VLAN IDs separated by a hyphen (for example 1,2,3-5). The range is from 1 to 4094.

- **default**—Specifies the list of the C-VLANs other than those not specified. If a default action is not configured the input frames with unspecified C-VLANs are dropped.
- ***outer-vlan-id*** —Specifies the added an outer S-VLAN tag. The range of the S-VLAN tag is 1 to 4094.
- **drop**—Specify that frames with the specified C-VLANs are dropped.

Default Configuration

No VLAN mapping is configured.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **switchport vlan-mapping tunnel** *vlan-list outer-vlan-id* command to configure selective tunneling for the given C-VLANs.

The S-VLAN specified by the *outer-vlan-id* argument must be created before configuring of this command. If this VLAN does not exist the command fails.

Use the **switchport vlan-mapping tunnel** *vlan-list* **drop** command to configure selective drop for the given C-VLANs.

Use the **switchport vlan-mapping tunnel default** *outer-vlan-id* command to configure tunneling for C-VLANs other than those not specified.

Use the **switchport vlan-mapping tunnel default drop** command to configure drop C-VLANs other than those not specified.

The **switchport vlan-mapping tunnel** command performs the following actions:

- Creates an ACL for mapping VLANs from *vlan-list* to *outer-vlan-id*, it has not been created.
- Adds to the ACL one rule for each VLAN from *vlan-list.*
- Reserves the place into TTI for this ACL. If there is not enough free place into TTI the command fails.

Note. The ACL can be bound on the interface later by the **vlan-mapping tunnel** command.

- **A**dds the edge interface to the VLAN specified by the *outer-vlan-id* argument.

The ACL contains V+1 rules, where:

- **V**—The number of specified C-VLANs.

A few **switchport vlan-mapping tunnel** commands can be defined on the same interface, only if their *vlan-list* arguments do not contain common VLAN-IDs.

Use the **no switchport vlan-mapping tunnel** *vlan-list* command to delete tunneling for the specified C-VLANs and remove the interface from the corresponding S-VLANs.

Use the **no switchport vlan-mapping tunnel default** command to delete the default tunneling and remove the interface from the corresponding S-VLANs.

Use the **no switchport vlan-mapping tunnel** command to delete tunneling for all C-VLANs and remove the interface from the corresponding S-VLANs.

Examples

Example 1 This example shows how to configure traditional tunnelling of all traffic on the port to a S-VLAN ID of 10:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel default 10
switchxxxxxx(config-if)# exit
```

Example 2 This example shows how to configure selective tunneling on the port so that traffic with a C-VLAN ID of 5, 7, or 8 would be tunneled with a S-VLAN ID of 100. The traffic of any other C-VLAN IDs is dropped:

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# switchport vlan-mapping tunnel 5,7-8 100
switchxxxxxx(config-if)# switchport vlan-mapping tunnel 12,27 5
switchxxxxxx(config-if)# switchport vlan-mapping tunnel default drop
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol vlan

To specify S-VLAN-ID used for encapsulation of forwarded untagged Layer 2 frames received on a vlan-mapping tunnel interface, use the **switchport vlan-mapping tunnel l2protocol vlan** command in Interface (Ethernet, Port Channel) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping tunnel l2protocol vlan *vlan-id*

no switchport vlan-mapping tunnel l2protocol vlan

Parameters

- ***vlan-id*** —Specifies S-VLAN-ID used to encapsulate of forwarded untagged Layer 2 frames.

Default Configuration

The VLAN_ID is not defined.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **switchport vlan-mapping tunnel l2protocol vlan** command, to specify S-VLAN-ID used for encapsulation of forwarded untagged Layer 2 frames received on a **vlan-mapping tunnel** interface. The S-VLAN ID can be that of an S-VLAN already defined on port or a new one

If the command is not configured the allowed untagged Layer 2 frames are not forwarded.

Example

The following example specifies the S-VLAN used for forwarding L2 frames:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol vlan 100
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol cos

To specify a class of service (CoS) value globally into S-VLAN tag of forwarded Layer 2 frames to the Provide network, use the **switchport vlan-mapping tunnel l2protocol cos** command in Global Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping tunnel l2protocol cos *cos-value*

no switchport vlan-mapping tunnel **l2protocol cos**

Parameters

- ***cos-value*** —Specifies the CoS value in range 0..7.

Default Configuration

The *cos-value* is 5.

Command Mode

Global Configuration mode

User Guidelines

Use the **switchport vlan-mapping tunnel l2protocol cos** command, to specify a class of service (CoS) value globally into S-VLAN tag of forwarded Layer 2 frames to the Provide network.

Use the **no switchport vlan-mapping tunnel l2protocol cos** command, to return to the default CoS.

Example

The following example specifies the cos of forwarded L2 frames:

```
switchxxxxxx(config)# switchport vlan-mapping tunnel l2protocol cos 6
```

switchport vlan-mapping tunnel l2protocol cos interface

To specify a class of service (CoS) value per interface into S-VLAN tag of forwarded Layer 2 frames to the Provide network, use the **switchport vlan-mapping tunnel l2protocol cos interface** command in Interface (Ethernet, Port Channel) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping tunnel l2protocol cos interface *cos-value*

vlan-mapping tunnel l2protocol cos interface

Parameters

- ***cos-value*** —Specifies the CoS value in range 0..7.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **switchport vlan-mapping tunnel l2protocol cos interface** command, to specify a class of service (CoS) value globally into S-VLAN tag of forwarded Layer 2 frames received on the given vlan-mapping tunnel edge interface and sent to the Provide network.

Use the **no switchport vlan-mapping tunnel l2protocol cos interface** command, to return to the default CoS on the given vlan-mapping tunnel edge interface.

Example

The following example specifies the cos of forwarded L2 tunneled frames:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol cos interface 6
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol drop-threshold

To specify the drop threshold for forwarded L2 packets that can be received on the given vlan-mapping tunnel edge interface (in kilobits per second), use the **switchport vlan-mapping tunnel l2protocol drop-threshold** command in Interface (Ethernet, Port Channel) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping tunnel l2protocol drop-threshold [disable | enable *committed-rate-kbps***]**

no switchport vlan-mapping tunnel l2protocol drop-threshold

Parameters

- **disable** - disable drop-threshold on interface
- **enable** - enable drop-threshold on interface
- ***committed-rate-kbps***—Specifies the threshold in kilobits per second (range 8-256)

Default Configuration

Drop-threshold is enabled and rate set to 32 kilobits per second.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the switchport vlan-mapping tunnel l2protocol drop-threshold command, to enable or disable drop threshold, and set the drop rate, for received forwarded L2 protocol frames on a given vlan-mapping tunnel edge interface. The frames exceeding this threshold are dropped.

The L2 protocol frames are protocol frames which are tunneled using command switchport vlan-mapping tunnel l2protocol forward, on page 1262.

Use the **no switchport vlan-mapping tunnel l2protocol drop-threshold** command, to return configuration to default - drop threshold enabled with rate of 32 kilobits per second.

Example

The following example sets the drop threshold to 16 kilobits per second:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol drop-threshold 16
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping tunnel l2protocol forward

To enable forward over the Provider network untagged Layer 2 frames received on a vlan-mapping tunnel interface, use the **switchport vlan-mapping tunnel l2protocol forward** command in Interface (Ethernet, Port Channel) Configuration mode. To restore the default configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping tunnel l2protocol forward [*protocol*]

no switchport vlan-mapping tunnel l2protocol forward [*protocol*]

Parameters

- ***protocol*** —Configures a protocol the command is applied. The argument may have one of the following values:
  - cdp
  - lldp
  - stp
  - vtp

If the *protocol* argument is not configured then the command is applied to all these protocols.

Default Configuration

The Layer 2 frames are not forwarded.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

By default, the switch drops on edge ports input L2 PDUs with the following destination MAC addresses:

- 01:80:C2:00:00:00-01:80:C2:00:00:FF - with the exception of LACP frame (destination MAC 01:80:C2:00:00:02) which **is processed** by the edge port
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
- 01:00:0C:CD:CD:D0

Use the **switchport vlan-mapping tunnel l2protocol forward** command to enable forward over the Provider network untagged frames of a given Layer 2 protocol received on a vlan-mapping tunnel interface. The received tagged Layer 2 frames are discarded.

When a L2 protocol is forwarded the switch overwrites the customer destination MAC address with a ’well-known’ Multicast address 01:00:0C:CD:CD:D0 before transmission the frame on non-edge port.

When a frame with the destination address equals to this well-known Multicast address is received on non-edge port the switch forwards it to all non-edge ports belonging to the S_VLAN and to all edge ports belonging to the S-VLAN and configured with the forward option for the given protocol.

The switch replaces the 'well-known’ destination MAC address with the respective Layer 2 protocol MAC address he respective Layer 2 protocol MAC address.

CDP cannot be both enabled and also tunneled on the same interfaces. To enable **CDP** tunneling on a Port Channel interface, **CDP** first needs to be disabled on **all** the members of the Port Channel (active and in-active). Likewise, an Ethernet Interface with CDP enabled cannot be added to a Port Channel on which CDP tunneling is enabled.

LLDP cannot be both enabled and also tunneled on the same interfaces. To enable **LLDP** tunneling on a Port Channel interface, **LLDP** first needs to be disabled on **all** the members of the Port Channel (active and in-active). Likewise, an Ethernet Interface with CDP enabled cannot be added to a Port Channel on which CDP tunneling is enabled.

If tunnel is defined, use the **no switchport vlan-mapping tunnel l2protocol forward** command without the *protocol* argument to return to the default treatment of all Layer 2 BPDUs.

Use the **no switchport vlan-mapping tunnel l2protocol forward** command with the *protocol* argument to return to the default treatment of the specified protocol BPDUs.

Example 1—The following example specifies that all the 4 protocols (CDP, LLDP, VTP and STP) frames will be forwarded:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol forward
switchxxxxxx(config-if)# exit
```

Example 2—The following example specifies that only CDP and LLDP protocols frames will be forwarded (Other 2 protocols frames of STP and VTP will be dropped):

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol forward cdp
switchxxxxxx(config-if)# switchport vlan-mapping tunnel l2protocol forward lldp
switchxxxxxx(config-if)# exit
```

switchport vlan-mapping one-to-one

To configure one-to-one VLAN translation on an edge interface, use the **switchport vlan-mapping one-to-one** command in Interface (Ethernet, Port Channel) Configuration mode. To delete the configuration, use the **no** form of this command.

Syntax

switchport vlan-mapping one-to-one *vlan-id translated-vlan-id*

no switchport vlan-mapping one-to-one [*vlan-id*]

Parameters

- ***vlan-id***—Specifies the external VLAN (E-VLAN) for one-to-one VLAN translation. The range is from 1 to 4094.
- ***translated-vlan-id*** —Specifies B-VLAN replacing the E-VLAN. The range is from 1 to 4094.

Default Configuration

No VLAN mapping is configured.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Use the **switchport vlan-mapping one-to-one** command to configure selective one-to-one VLAN translation.

The S-VLAN specified by the *translated-vlan-id* argument must be created before configuring of this command. If this VLAN does not exist the command fails.

A few **switchport vlan-mapping one-to-one** commands with different arguments can be defined on the same interface.

In the vlan-mapping one-to-one mode an interface belongs to all S-VLANs for which mapping on this interface is defined as egress tagged interface. The interface PVID is set to 4095.

In the vlan-mapping one-to-one mode an interface uses one ingress ACL and one egress ACL. The **switchport vlan-mapping one-to-one** command adds rules to this ACLs. These

ACLs are applied in order to:

- Ingress ACL (in TTI):
  - Replace specified C-VLAN-ID by S-VLAN-ID.
  - Drop frames with unspecified C-VLAN-IDs.

    - Drop untagged input frames.

- Egress ACL (in TCAM):
    - Replace S-VLAN-ID by C-VLAN-ID.

The **switchport vlan-mapping one-to-one** command adds rules to these ACLs and they are bound on the interface only if its mode is vlan-mapping one-to-one.

The ingress ACL contains V+1 rules and the egress ACL contains V rules, where

- **V**—The number of specified C-VLANs.

Use the **no switchport vlan-mapping one-to-one** *vlan-id* command to delete the one-to-one VLAN translation configuration for the given E-VLAN.

Use the **no switchport vlan-mapping one-to-one** command to delete all VLAN one-to-one translations.

Example

This example shows how to configure one-to-one VLAN translation on a port:

```
switchxxxxxx(config)# interface gi1/0/1
switchxxxxxx(config-if)# switchport vlan mapping one-to-one 5 105
switchxxxxxx(config-if)# switchport vlan mapping one-to-one 15 5
switchxxxxxx(config-if)# switchport vlan mapping one-to-one 105 225
switchxxxxxx(config-if)# exit
```

map protocol protocols-group

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 . 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 Database Configuration mode

User Guidelines

Forwarding of packets based on their protocol requires setting up groups of protocols and then mapping these groups to VLANs.

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
```

switchport general map protocols-group vlan

Use the **switchport general map protocols-group vlan** Interface Configuration 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** command (range: 1–65535).
- ***vlan-id***—Defines the VLAN ID in the classifying rule.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The VLAN classification rule priorities are:

- MAC-based VLAN (best match among the rules)
- Subnet-based VLAN (best match among the rules)
- Protocol-based VLAN
- 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
```

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

Command Mode

User 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

map mac macs-group

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. 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-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.
- ***group***—Specifies the group number (range: 1–2147483647)

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their MAC address requires setting up groups of MAC addresses and then mapping these groups to VLANs.

Up to 256 MAC addresses (host or range) can be mapped to one or many MAC-based VLAN groups.

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 gi1/0/4
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
```

switchport general map macs-group vlan

Use the **switchport general map macs-group vlan** Interface Configuration 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

- **group**—Specifies the group number (range: 1–2147483647)
- ***vlan-id***—Defines the VLAN ID associated with the rule.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

MAC-based VLAN rules cannot contain overlapping ranges on the same interface.

The VLAN classification rule priorities are:

- MAC-based VLAN (best match among the rules)
- Subnet-based VLAN (best match among the rules)
- Protocol-based VLAN
- PVID

User Guidelines

Each MAC address (host or range) in the MAC-based group assigned to an interface consumes a single TCAM entry.

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 gi1/0/4
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
```

show vlan macs-groups

Use the **show vlan macs-groups** EXEC mode command to display the MAC addresses that belong to the defined MAC-based classification rules.

Syntax

show vlan macs-groups

Default Configuration

Command Mode

User EXEC mode

Example

The following example displays defined MAC-based classification rules.

```
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
```

map subnet subnets-group

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.
- ***group***—Specifies the group number. (range: 1–2147483647)

Command Mode

VLAN Database Configuration mode

User Guidelines

Forwarding of packets based on their IP subnet requires setting up groups of IP subnets and then mapping these groups to VLANs.

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-vlan)# switchport general map subnets-group 4 vlan 8
```

switchport general map subnets-group vlan

Use the **switchport general map subnets-group vlan** Interface Configuration 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.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The VLAN classification rule priorities are:

- MAC-based VLAN (Best match among the rules)
- Subnet-based VLAN (Best match among the rules)
- Protocol-based VLAN
- 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-vlan)# switchport general map subnets-group 4 vlan 8
```

show vlan subnets-groups

Use the **show vlan subnets-groups** EXEC mode command to display subnets-groups information.

Syntax

show vlan subnets-groups

Command Mode

User 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
```

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: Ethernet port or port-channel.

Command Mode

Privileged EXEC mode

Default

Displays the status of all interfaces.

User Guidelines

Each port mode has its own private configuration. The **show interfaces switchport** command displays all these configurations, but only the port mode configuration that corresponds to the current port mode displayed in "Administrative Mode" is active.

Example

```
switchxxxxxx# show interfaces switchport gi1/0/1
Gathering information...
S-VLAN Ethernet Type: 0x88a8 (802.1ad)
VLAN Mapping Tunnel L2 protocols Global CoS: 6
Name: gi1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: down
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1
                2-4094 (Inactive)
General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: Enabled
General GVRP VLANs: none
Customer Mode VLAN: none
VLAN Mapping Tunnel:
S-VLAN Ethernet Type: 0x8100 (802.1q)
C-VLANs                 Outer S-VLAN
--------------------    ------------
```

```
2                       12
12,16-18                100
default                 1100
VLAN Mapping Tunnel L2 protocols S-VLAN: 100
VLAN Mapping Tunnel L2 protocols Interface CoS: 6 (global)
VLAN Mapping Tunnel L2 protocols forward enabled: cdp,stp
Drop Threshold: 4 kbps (default)
VLAN Mapping One-to-one:
C-VLANs                 Translated S-VLAN
--------------------    ----------------------
2                       102
12                      112
100                     10
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none
Protected: Enabled, Uplink is gi1/0/1
Classification rules:
Classification Type   Group ID   VLAN ID
-------------------   --------   -------
Protocol                   1        19
Protocol                   1        20
Protocol                   2        72
Subnet                     1        15
MAC                        1        77
```

private-vlan

Use the **private-vlan** Interface VLAN Configuration mode command to configure a private VLAN. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

Syntax

private-vlan {**primary** | **community** | **isolated**}

no private-vlan

Parameters

- **primary**—Designate the VLAN as a primary VLAN.
- **community**—Designate the VLAN as a community VLAN.
- **isolated**—Designate the VLAN as an isolated VLAN.

Default Configuration

No private VLANs are configured.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

- The VLAN type cannot be changed if there is a private VLAN port that is a member in the VLAN.

- The VLAN type cannot be changed if it is associated with other private VLANs.
- The VLAN type is not kept as a property of the VLAN when the VLAN is deleted.

Example

The following example set vlan 2 to be primary vlan:

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# private-vlan primary
```

private-vlan association

Use the **private-vlan association** Interface VLAN Configuration mode command to configure the association between the primary VLAN and secondary VLANs. Use the **no** form of this command to remove the association.

Syntax

private-vlan association [**add** | **remove**] *secondary-vlan-list*

no private-vlan association

Parameters

- **add** *secondary-vlan-list*—List of VLAN IDs of type secondary to add to a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.This is the default action.
- **remove** secondary-vlan-list—List of VLAN IDs of type secondary to remove association from a primary VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs.

Default Configuration

No private VLANs are configured.

Command Mode

Interface (VLAN) Configuration mode

User Guidelines

- The command can only be executed in the context of the primary VLAN.
- A private VLAN cannot be removed or have its type changed, if it is associated with other private VLANs.
- A primary VLAN can be associated with only a single, isolated VLAN.
- A secondary VLAN can be associated with only one primary VLAN.
- The association of secondary VLANs with a primary VLAN cannot be removed if there are private VLAN ports that are members in the secondary VLAN.

- In MSTP mode, all the VLANs that are associated with a private VLAN must be mapped to the same instance.

Example

The following example associate secondary VLAN 20,21,22 and 24 to primary VLAN 2.

```
switchxxxxxx(config)# interface vlan 2
switchxxxxxx(config-if)# private-vlan association add 20-22,24
```

switchport private-vlan mapping

Use the **switchport private-vlan mapping** Interface Configuration mode command to configure the VLANs of the private VLAN promiscuous port. Use the **no** form of this command to reset to default.

Syntax

switchport private-vlan mapping *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*

no switchport private-vlan mapping

Parameters

- ***primary-vlan-id*** —The VLAN ID of the primary VLAN.
- **add** secondary-vlan-list—Specifies one or more secondary VLANs to be added to the port.
- **remove** secondary-vlan-list—Specifies one or more secondary VLANs to be removed from the port.

Default Configuration

No VLAN is configured.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The secondary VLANs should be associated with the primary VLANs, otherwise the configuration is not accepted.

Example

The following example add promiscuous port gi1/0/4 to primary VLAN 10 and to secondary VLAN 20.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport private-vlan mapping 10 add 20
```

switchport private-vlan host-association

Use the **switchport private-vlan host-association** Interface Configuration mode command to configure the association of a host port with primary and secondary VLANs of the private VLAN. Use the **no** form of this command to reset to default.

Syntax

switchport private-vlan host-association *primary-vlan-id secondary-vlan-id*

no switchport private-vlan host-association

Parameters

- ***primary-vlan-id***—The VLAN ID of the primary VLAN.
- ***secondary-vlan-id***—Specifies the secondary VLAN.

Default Configuration

No association.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

The secondary VLAN must be associated with the primary VLAN, otherwise the configuration is not accepted. See the **private-vlan association** command.

The port association configuration depends on the type of the secondary VLAN.

The port association configuration for a community secondary VLAN includes:

- The port is added as untagged to the primary VLAN and to the secondary VLAN.
- The PVID is set to the VLAN-ID of the secondary VLAN.
- The port ingress filtering is enabled.

The port association configuration for an isolated secondary VLAN includes:

- The port is added as untagged only to the primary VLAN and is not added to the secondary VLAN.
- The PVID is set to the VLAN-ID of the secondary VLAN.
- The port ingress filtering is disabled.

Example

The following example set port gi1/0/4 to secondary VLAN 20 in primary VLAN 10.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport private-vlan host-association 10 20
```

show vlan private-vlan

Use the **show vlan private-vlan** EXEC mode command to display private VLAN information.

Syntax

show vlan private-vlan [**tag** *vlan-id*]

Parameters

- **tag** vlan-id—Primary VLAN that represent the private VLAN to be displayed.

Default Configuration

All private VLANs are displayed.

Command Mode

User EXEC mode

User Guidelines

The **show vlan private-vlan** command does not include non-private VLAN ports that are members in private VLANs. Tag parameters of non-primary VLAN will result in an empty show output.

Example

```
switchxxxxxx# show vlan private-vlan
  Primary    Secondary     Type             Ports
----------- ----------- ----------- ----------------------
    150                   primary           gi1/0/1
    150         151       isolated          gi1/0/2
    160                   primary           gi1/0/3
    160         161       community         gi1/0/4
switchxxxxxx# show vlan private-vlan 150
  Primary    Secondary     Type             Ports
----------- ----------- ----------- ----------------------
    150                   primary           gi1/0/1
    150         151       isolated          gi1/0/4
```

switchport access multicast-tv vlan

To assign a Multicast-TV VLAN to an access port, use the **switchport access multicast-tv vlan** command in Interface (Ethernet, Port Channel) Configuration mode. To return to the default, use the **no** format of the command.

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 (Ethernet, Port Channel) Configuration mode

User Guidelines

When the port is assigned to a different Multicast-TV VLAN, it is automatically removed from its previous VLAN and added it to the new Multicast-TV VLAN.

When an existed Multicast-TV VLAN is assigned to an access port, the multicast messages received on a membership of the Multicast-TV VLAN are forwarded to the access port. All messages received on the access port are bridged only into its Access VLAN.

Example

The following example enables gi1/0/4 to receive Multicast transmissions from VLAN 11.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport access multicast-tv vlan 11
```

switchport customer multicast-tv vlan

To assign Multicast-TV VLANs to a customer port, use the **switchport customer multicast-tv vlan** command in Interface (Ethernet, Port Channel) Configuration mode. To return to the default, use the **no** format of the command.

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 (Ethernet, Port Channel) Configuration mode

User Guidelines

When an existed Multicast-TV VLAN is assigned to a customer port, the multicast messages received on a membership of the Multicast-TV VLAN are forwarded to the customer port. All messages received on the customer port are not bridged only into the Multicast-TV VLAN.

Example

The following example enables gi1/0/4 to receive Multicast transmissions from VLANs 5, 6, 7.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# switchport customer multicast-tv vlan add 5-7
```

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.

Command Mode

User 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
------------        ----------------------
gi1/0/3, gi1/0/4    gi1/0/1-2
```

vlan prohibit-internal-usage

Use the **vlan prohibit-internal-usage** command in Global configuration mode to specify VLANs that cannot be used by the switch as internal VLANs.

Syntax

vlan prohibit-internal-usage none | {add | except | remove} *vlan-list*

Parameters

- **none**—The Prohibit Internal Usage VLAN list is empty: any VLAN can be used by the switch as internal.
- **except**—The Prohibit Internal Usage VLAN list includes all VLANs except the VLANs specified by the *vlan-list* argument: only the VLANs specified by the *vlan-list* argument can be used by the switch as internal.
- **add**—Add the given VLANs to the Prohibit Internal Usage VLAN list.
- **remove**—Remove the given VLANs from the Prohibit Internal Usage VLAN list.
- ***vlan-list***—List of VLAN. Separate nonconsecutive VLAN IDs with a comma and no spaces. Use a hyphen to designate a range of IDs. The VLAN ID that can be used is from 1 through 4094.

Default Configuration

The Prohibit Internal usage VLAN list is empty.

Command Mode

Global Configuration mode

User Guidelines

The switch requires an internal VLAN in the following cases:

- One VLAN for each IP interface is defined directly on an Ethernet port or on a Port channel.
- One VLAN for each IPv6 tunnel.
- One VLAN for 802.1x.

When a switch needs an internal VLAN it takes a free VLAN with the highest VLAN ID.

Use the **vlan prohibit-internal-usage** command to define a list of VLANs that cannot be used as internal VLANs after reload.

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

- Add the VLAN to the Prohibited User Reserved VLAN list.
- Copy the Running Configuration file to the Startup Configuration file
- Reload the switch
- Create the VLAN

Example 1—The following example specifies that VLANs 4010, 4012, and 4090-4094 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage add 4010,4012,4090-4094
```

Example 2—The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage all
vlan prohibit-internal-usage remove 4000-4107
```

Example 3—The following specifies that all VLANs except 4000-4107 cannot be used as internal VLANs:

```
vlan prohibit-internal-usage 4000-4107
```

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

Command Mode

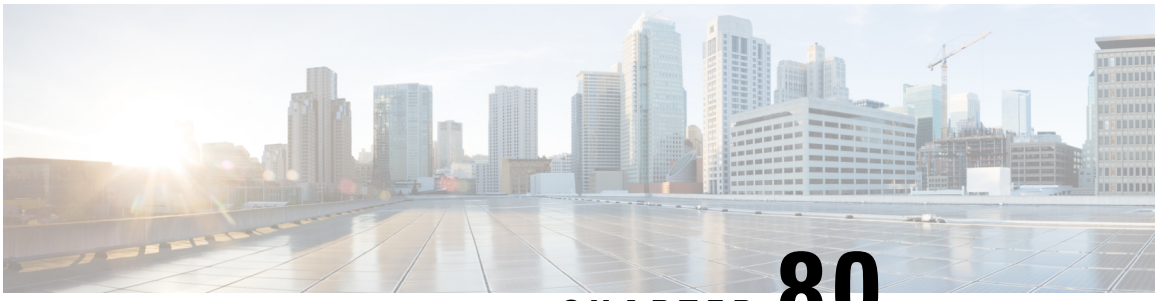
Privileged EXEC mode

Example

The following example displays VLANs used internally by the switch:

show vlan internal usage

```
User Reserved VLAN list after reset: 4010,4012,4080-4094
Current User Reserved VLAN list: 4010,4012,4090-4094
VLAN   Usage
----   --------
4089   gi1/0/2
4088   gi1/0/3
4087   tunnel 1
4086   802.1x
```



CHAPTER 80

Voice VLAN Commands

This chapter contains the following sections:

- show voice vlan, on page 1283
- show voice vlan local, on page 1286
- voice vlan state, on page 1287
- voice vlan refresh, on page 1288
- voice vlan id, on page 1289
- voice vlan vpt, on page 1290
- voice vlan dscp, on page 1291
- voice vlan oui-table, on page 1291
- voice vlan cos mode, on page 1293
- voice vlan cos, on page 1293
- voice vlan aging-timeout, on page 1294
- voice vlan enable, on page 1294

show voice vlan

To display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI, use the **show voice vlan** Privileged EXEC mode command.

Syntax

show voice vlan [**type** {***oui*** [{*interface-id* | **detailed**}] | *auto*}]

Parameters

- **type oui**—(Optional) Common and OUI-voice-VLAN specific parameters are displayed.
- **type auto**—(Optional) Common and Auto Voice VLAN-specific parameters are displayed.
- **interface-id**—(Optional) Specifies an Ethernet port ID.
- **detailed**—(Optional) Displays information for non-present ports in addition to present ports.

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 present interfaces is displayed. If detailed is used, non-present ports are also displayed.

Command Mode

Privileged EXEC mode

User Guidelines

Using this command without parameters displays the current voice VLAN type parameters and local and agreed voice VLAN settings.

Using this command with the **type** parameter displays the voice VLAN parameters relevant to the type selected. The the local and agreed voice VLAN settings are displayed only if this is the current voice VLAN state.

The interface-id parameter is relevant only for the OUI VLAN type.

Examples

The following examples display the output of this command in various configurations.

Example 1—Displays the **auto** voice VLAN parameters (this is independent of the voice VLAN state actually enabled).

```
switch>show voice vlan type auto
switchxxxxxx# show voice vlan type auto
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
switchxxxxxx#
```

Example 2—Displays the current voice VLAN parameters when the voice VLAN state is auto-enabled.

```
switch>show voice vlan
Administrate Voice VLAN state is auto-enabled on IPv4
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 16:48:13
switchxxxxxx#
```

Example 3—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered but voice VLAN has not been triggered.

```
switch>show voice vlan
Administrate Voice VLAN state is auto-triggered on ipv6
Operational Voice VLAN state is disabled
VSDP Authentication is disabled
```

Example 4—Displays the current voice VLAN parameters when the administrative voice VLAN state is auto-triggered and it has been triggered.

```
switchxxxxxx(config)# voice vlan state auto-triggered
switchxxxxxx(config)# voice vlan state auto-triggered
operational voice vlan state is auto
admin state is auto triggered
switchxxxxxx# show voice vlan
Administrate Voice VLAN state is auto-triggered on ipv6
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Agreed Voice VLAN is received from switch 00:24:01:30:10:00
Agreed Voice VLAN priority is  0 (active static source)
Agreed Voice VLAN-ID is 5
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Jul-11 15:52:51
```

Example 5—Displays the current voice VLAN parameters when both auto voice VLAN and OUI are disabled.

```
switch>show voice vlan
switchxxxxxx# show voice vlan
Administrate Voice VLAN state is disabled
Operational Voice VLAN state is disabled
Best Local Voice VLAN-ID is 5
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
Aging timeout: 1440 minutes
```

Example 6—Displays the voice VLAN parameters when the voice VLAN operational state is OUI.

```
switch>show voice vlan
Administrate Voice VLAN state is oui-enabled
Operational Voice VLAN state is oui-enabled
Best Local Voice VLAN-ID is 1 (default)
Best Local VPT is 4
Best Local DSCP is 1
Aging timeout: 1440 minutes
CoS: 6
Remark: Yes
OUI table
MAC Address - Prefix   Description
--------------------   ------------------
00:E0:BB               3COM
00:03:6B               Cisco
00:E0:75               Veritel
00:D0:1E               Pingtel
00:01:E3               Simens
00:60:B9               NEC/Philips
00:0F:E2               Huawei-3COM
00:09:6E               Avaya
Interface        Enabled    Secure    Activated  CoS Mode
-------------    -------    -------   ---------  --------
gi1/0/1              Yes        Yes         Yes       all
gi1/0/2              Yes        Yes         No        src
gi1/0/3              No         No
...
```

show voice vlan local

The **show voice vlan local** Privileged EXEC mode command displays information about the auto voice VLAN local configuration, including the best local voice VLAN.

Syntax

show voice vlan local

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Examples

Example 1—A CDP device is connected to an interface and a conflict is detected:

```
30-Apr-2011 00:39:24 %VLAN-W-ConflictingCDPDetected: conflict detected between operational
 VLAN and new CDP device 00:1e:13:73:3d:62 on interface gi7. Platform TLV is -4FXO-K9, Voice
 VLAN-ID is 100...
switchxxxxxx# show voice vlan local
Administrate Voice VLAN state is auto-triggered on IPv6
Operational Voice VLAN state is auto-enabled
VSDP Authentication is enabled, key string name is alpha
The character '*; marks the best local Voice VLAN
VLAN-ID  VPT    DSCP   Source        MAC Address         Interface
-------- -----  -----  ---------     -----------         ------------
   1       5     46    default       ---                 ---
  *104     7     63    static        ---                 ---
   100                 CDP           00:1e:13:73:3d:62   gi1/0/4
```

Example 2—Displays the local voice VLAN configuration when the voice VLAN state is auto-triggered.

```
switchxxxxxx# show voice vlan local
Administrate Voice VLAN state is auto-triggered on IPv4
Operational Voice VLAN state is auto-enabled
 VLAN-ID   VPT   DSCP    Source        MAC Address       Interface
--------- ----- ------ ---------- -------------------- -----------
    1       5     46    default            ---              ---
  *100                    CDP       00:23:56:1a:dc:68     gi1/0/4   100
 CDP       00:44:55:44:55:4d     gi1/0/4
The character "*" marks the best local voice VLAN.
```

Example 3—Displays the local voice VLAN configuration when the voice VLAN state is OUI.

```
switchxxxxxx# show voice vlan local
Administrate Voice VLAN state is auto-OUI
Operational Voice VLAN state is OUI
The character '*; marks the best local Voice VLAN
VLAN-ID    VPT   DSCP   Source      MAC Address      Interface
---------  ----  -----  ---------   ------------     --------------------
       1    0     0     default        ---               ---
     *10    1     27    static         ---               ---
      10                CDP          00:00:12:ea:87:dc    gi1/0/1
      10                CDP          00:00:aa:aa:89:dc    po1
```

voice vlan state

To set the type of voice VLAN that is functional on the device or disable voice VLAN entirely, use the **voice vlan state** Global Configuration mode command.

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

Syntax

voice vlan state {***auto-enabled*** **|** ***auto-triggeredoui-enabled*** | ***disabled***}

no voice vlan state

Parameters

- **auto-enabled**—Auto Voice VLAN is enabled.
- **auto-triggered**—Auto Voice VLAN on the switch is in standby and is put into operation when the switch detects a CDP device advertising a voice VLAN or if a voice VLAN ID is configured manually on the switch.
- **oui-enabled**—Voice VLAN is of type OUI.
- **disabled**—Voice VLAN is disabled.

Default Configuration

Disabled

Command Mode

Global Configuration mode

User Guidelines

By factory default, CDP, LLDP, and LLDP-MED are enabled on the switch. In addition, manual Smartport mode and Basic QoS with trusted DSCP is enabled.

All ports are members of default VLAN 1, which is also the default Voice VLAN.

If the state is set to dynamic voice VLAN (**auto-triggered**) mode then voice VLAN is enabled by a trigger (advertisement received by voice device attached to port).

If the administrative state is:

- **disabled** — The operational state is **disabled**.
- **oui-enabled** —The operational state is **oui-enabled**.
- **auto-enabled** — The operational state is **auto-enabled**.
- **auto-triggered** — The operational state is **auto-enabled** only if one of the following occurs:
  - A static local configured voice VLAN ID, CoS/802.1p, and/or DSCP that is not factory default is configured.

- A CDP voice VLAN advertisement is received from a neighboring CDP device that is not a a device of the same family as the current device.
- A Voice Service Discovery Protocol (VSDP) message was received from a neighbor switch. VSDP is a Cisco Small Business proprietary protocol for SF and SG series managed switches.
- In all other cases the operational state is **disabled**.

Notes:

- To change the administrative state from **oui-enabled** to **auto-enabled** (or **auto-triggered)**, or vice versa, you must first set the administrative state to **disabled**.
- The administrative state cannot be set to **oui-enabled** if the Auto SmartPort administrative state is **enabled**.
- The administrative state cannot be set to **oui-enabled** if the voice VLAN is the default VLAN (VLAN 1). For **oui-enabled** mode, the voice VLAN cannot be 1.

Examples

Example 1 —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>
```

Example 2 — The following example disables the Voice VLAN state. All auto Smartport configuration on ports are removed.

```
switchxxxxxx(config)# voice vlan state disabled
All interfaces with Auto Smartport dynamic type will be set to default.
Are you sure you want to continue? (Y/N)[Y] Y
switchxxxxxx(config)# 30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 5
30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 8
30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 9
30-Apr-2011 00:04:41 %LINK-W-Down:  Vlan 100
```

Example 3 —The following example sets the Voice VLAN state to auto-triggered. The VLANs are re-activated after auto SmartPort state is applied.

```
switchxxxxxx(config)# voice vlan state auto-triggered
switchxxxxxx(config)# 30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 5
30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 8
30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 9
30-Apr-2011 00:13:52 %LINK-I-Up:  Vlan 100
```

voice vlan refresh

To restart the Voice VLAN discovery process on all the Auto Voice VLAN-enabled switches in the VLAN by removing all externally learned voice VLAN attributes and resetting the voice VLAN to the default voice VLAN, use the **voice vlan refresh** Global Configuration mode command.

Syntax

voice vlan refresh

Parameters

This command has no arguments or keywords

Default Configuration

None

Command Mode

Global Configuration mode

Example

```
switchxxxxxx(config)# voice vlan refresh
switchxxxxxx(config)#
30-Apr-2011 02:01:02 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by VSDP. Voice VLAN-ID
100, VPT 5, DSCP 46 (Notification that Agreed Voice VLAN is updated)
(Auto Smartport configuration is changed)
30-Apr-2011 02:01:05 %LINK-W-Down:  Vlan 50
30-Apr-2011 02:01:05 %LINK-W-Down:  Vlan 100
30-Apr-2011 02:01:06 %LINK-I-Up:  Vlan 50
30-Apr-2011 02:01:06 %LINK-I-Up:  Vlan 100
switchxxxxxx# show voice vlan
Administrate Voice VLAN state is auto-triggered
Operational Voice VLAN state is auto-enabled
Best Local Voice VLAN-ID is 100
Best Local VPT is 5 (default)
Best Local DSCP is 46 (default)
(Following is the new active source)
Agreed Voice VLAN is received from switch b0:c6:9a:c1:da:00
Agreed Voice VLAN priority is  2 (active CDP device)
Agreed Voice VLAN-ID is 100
Agreed VPT is 5
Agreed DSCP is 46
Agreed Voice VLAN Last Change is 11-Apr-30 02:01:02
```

voice vlan id

To statically configure the VLAN identifier of the voice VLAN, use the **voice vlan id** Global Configuration mode command. To return the voice VLAN to the default VLAN (1), use the **no** format of the command.

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 35 was created.
switchxxxxxx(config)# 30-Apr-2011 00:19:51 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by
 VSDP. Voice VLAN-ID 35, VPT 5, DSCP 46
```

voice vlan vpt

To specify a value of VPT (802.1p VLAN priority tag) that will be advertised by LLDP in the Network Policy TLV, use the **voice vlan vpt** Global Configuration mode command. To return the value to the default, use the **no** format of the command.

Syntax

voice vlan vpt *vpt-value*

no voice vlan vpt

Parameters

vpt *vpt-value*—The VPT value to be advertised (range 0-7).

Default Configuration

5

Command Mode

Global Configuration mode

Example

The following example sets 7 as the voice VLAN VPT. A notification that the new settings are different than the old ones is displayed.

```
switchxxxxxx(config)# voice vlan vpt 7
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCPwill cause the
switch to advertise the administrative voice VLAN as static voice VLANwhich has higher
priority than voice VLAN learnt from external sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:24:52 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN
configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 5, DSCP 46
switchxxxxxx(config)# 30-Apr-2011 00:25:07 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by
 VSDP. Voice VLAN-ID 104, VPT 7, DSCP 46
```

voice vlan dscp

To specify a value of DSCP that will be advertised by LLDP in the Network Policy TLV, use the **voice vlan dscp** Global Configuration mode command. To return the value to the default, use the **no** format of the command.

Syntax

voice vlan dscp *dscp-value*

no voice vlan dscp

Parameters

dscp *dscp-value*—The DSCP value (range 0-63).

Default Configuration

46

Command Mode

Global Configuration mode

Example

The following example sets 63 as the voice VLAN DSCP.

```
switchxxxxxx(config)# voice vlan dscp 63
For Auto Voice VLAN, changes in the voice VLAN ID, CoS/802.1p, and/or DSCPwill cause the
switch to advertise the administrative voice VLAN as static voice VLANwhich has higher
priority than voice VLAN learnt from external sources.
Are you sure you want to continue? (Y/N)[Y] Y
30-Apr-2011 00:31:07 %VLAN-W-BestLocal!=Oper: inconsistency detected, VSDP voice VLAN
configuration differs from best local. Best local is Voice VLAN-ID 104, VPT 7, DSCP 46
switchxxxxxx(config)# 30-Apr-2011 00:31:22 %VLAN-I-ReceivedFromVSDP: Voice VLAN updated by
 VSDP. Voice VLAN-ID 104, VPT 7, DSCP 63
```

voice vlan oui-table

To configure the voice OUI table, use the **voice vlan oui-table** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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**—(Optional) 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
00:01:e3	Siemens AG Phone
00:03:6b	Cisco Phone
00:09:6e	Avaya Phone
00:0f:e2	Huawei-3COM Phone
00:60:b9	NEC/Philips Phone
00:d0:1e	Pingtel Phone
00:e0:75	Veritel Polycom Phone
00:e0:bb	3COM 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 experimental
```

voice vlan cos mode

To select the OUI voice VLAN Class of Service (CoS) mode, use the **voice vlan cos mode** Interface Configuration mode command. To return to the default, use the **no** form of this command.

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.
- **all**—QoS attributes are applied to packets that are classified to the Voice VLAN.

Default Configuration

The default mode is **src**.

Command Mode

Interface Configuration mode

Example

The following example applies QoS attributes to voice packets.

```
switchxxxxxx(config-if)# voice vlan cos mode all
```

voice vlan cos

To set the OUI Voice VLAN Class of Service (CoS), use the **voice vlan cos** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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**—(Optional) Specifies that the L2 user priority is remarked with the CoS value.

Default Configuration

The default CoS value is 6.

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
```

voice vlan aging-timeout

To set the OUI Voice VLAN aging timeout interval, use the **voice vlan aging-timeout** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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
```

voice vlan enable

To enable OUI voice VLAN configuration on an interface, use the **voice vlan enable** Interface Configuration mode mode command. To disable OUI voice VLAN configuration on an interface, use the **no** form of this command.

Syntax

voice vlan enable

no voice vlan enable

Parameters

This command has no arguments or keywords.

Default Configuration

Disabled

Command Mode

Interface Configuration mode

User Guidelines

This command is applicable only if the voice VLAN state is globally configured as OUI voice VLAN (using show voice vlan, on page 1283).

The port can join the voice VLAN only if it is member of in the PVID/native VLAN ID.

The port is added to the voice VLAN if a packet with a source MAC address OUI address (defined by voice vlan oui-table, on page 1291) is trapped on the port. Note: The packet VLAN ID does not have to be the voice VLAN, it can be any VLAN.

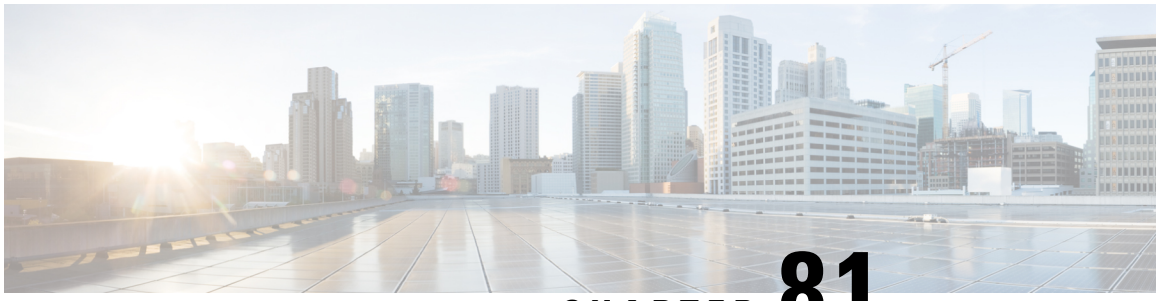
The port joins the voice VLAN as a tagged port.

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, on page 1294), the interface is removed from the voice VLAN.

Example

The following example enables OUI voice VLAN configuration on gi1/0/2.

```
switchxxxxxx(config)# interface gi1/0/2
switchxxxxxx(config-if)# voice vlan enable
```



CHAPTER 81

Web Server Commands

This chapter contains the following sections:

- ip https certificate, on page 1297
- ip https logging, on page 1298
- ip http port, on page 1298
- ip http server, on page 1299
- ip http secure-server , on page 1299
- ip http timeout-policy , on page 1300
- show ip http, on page 1301
- show ip https, on page 1301

ip https certificate

To configure the active certificate for HTTPS, use the **ip https certificate** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

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

Example

The following example configures the active certificate for HTTPS.

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

ip https logging

To enable or disable the logging of HTTPS session setup and tear down, use the ip https logging command in Global Configuration mode. To restore the default setting, use the no form of this command.

Syntax

ip https logging {enable| disable}

no ip https logging

Parameters

- **enable** — Enables HTTPS logging on device
- **disable** — disables HTTPS logging on device

Default Configuration

HTTPS session logging is disabled by default.

Command Mode

Global Configuration mode.

User Guidelines

This command enables HTTPS logging on the device. HTTPS logging is a mean to track the progress of HTTPS session setup and tear-down. HTTPS session setup and tear-down progress is tracked using SYSLOG message which are generated as part of the process. If HTTPS logging is disabled then SYSLOG messages will not be generated as part of the SSH setup or tear-down process.

Example

The following example enables HTTPS logging on the device.

```
switchxxxxxx(config)# ip https logging enable
```

ip http port

To specify the TCP port used by the web browser interface, use the **ip http port** Global Configuration mode command. To restore the default configuration, use the **no** form of this command.

Syntax

ip http port *port-number*

no ip http port

Parameters

port *port-number*—For use by the HTTP server. (Range: 1–59999)

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
```

ip http server

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

Syntax

ip http server

no ip http server

Parameters

This command has no arguments or keywords.

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
```

ip http secure-server

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

Syntax

ip http secure-server

no ip http secure-server

Parameters

This command has no arguments or keywords.

Default Configuration

Enabled

Command Mode

Global Configuration mode

Example

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

ip http timeout-policy

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

Syntax

ip http timeout-policy *idle-seconds* [{**http-only** | **https-only**}]

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)
- **http-only**—(Optional) The timeout is specified only for http
- **https-only**—(Optional) The timeout is specified only for https

Default Configuration

600 seconds. setting is applied for both HTTP and HTTPS

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
```

show ip http

To display the HTTP server configuration, use the **show ip http** Privileged EXEC mode command.

Syntax

show ip http

Parameters

This command has no arguments or keywords.

Command Mode

Privileged EXEC mode

Example

The following example displays the HTTP server configuration.

```
switchxxxxxx# show ip http
HTTP server enabled
Port: 80
Interactive timeout: 10 minutes, 0 seconds
```

show ip https

To display the HTTPS server configuration, use the **show ip https** Privileged EXEC mode command.

Syntax

show ip https

Parameters

This command has no arguments or keywords.

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, 0 seconds)
https session logging is disabled
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
```