



IPv6 Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 2960-X Switches)

First Published: June 27, 2014

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

Text Part Number: OL-32548-01



CONTENTS

Preface

Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 5

No and Default Forms of Commands 5

CLI Error Messages 5

Configuration Logging 6

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 7

Recalling Commands 7

Disabling the Command History Feature 8

Enabling and Disabling Editing Features 8

Editing Commands Through Keystrokes 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI on a Switch Stack 12

Accessing the CLI Through a Console Connection or Through Telnet 12

CHAPTER 2

Configuring IPv6 Unicast Routing 15

Finding Feature Information 15

Information About Configuring IPv6 Host Functions	15
Understanding IPv6	16
IPv6 Addresses	16
Supported IPv6 Unicast Routing Features	17
128-Bit Wide Unicast Addresses	17
DNS for IPv6	17
ICMPv6	17
Neighbor Discovery	18
IPv6 Stateless Autoconfiguration and Duplicate Address Detection	18
IPv6 Applications	18
Dual IPv4 and IPv6 Protocol Stacks	18
SNMP and Syslog Over IPv6	19
HTTP(S) Over IPv6	20
IPv6 and Switch Stacks	20
Default IPv6 Configuration	21
Configuring IPv6 Addressing and Enabling IPv6 Routing	21
Configuring IPv6 ICMP Rate Limiting (CLI)	23
Configuring Static Routing for IPv6 (CLI)	24
Displaying IPv6	26
Configuration Examples for IPv6 Unicast Routing	28
Configuring IPv6 Addressing and Enabling IPv6 Routing: Example	28
Configuring IPv6 ICMP Rate Limiting: Example	28
Configuring Static Routing for IPv6: Example	28
Displaying IPv6: Example	29

CHAPTER 3

Configuring MLD Snooping	31
Finding Feature Information	31
Information About Configuring IPv6 MLD Snooping	31
Understanding MLD Snooping	32
MLD Messages	33
MLD Queries	33
Multicast Client Aging Robustness	34
Multicast Router Discovery	34
MLD Reports	34
MLD Done Messages and Immediate-Leave	34

Topology Change Notification Processing	35
MLD Snooping in Switch Stacks	35
How to Configure IPv6 MLD Snooping	36
Default MLD Snooping Configuration	36
MLD Snooping Configuration Guidelines	36
Enabling or Disabling MLD Snooping on the Switch (CLI)	37
Enabling or Disabling MLD Snooping on a VLAN (CLI)	38
Configuring a Static Multicast Group (CLI)	39
Configuring a Multicast Router Port (CLI)	40
Enabling MLD Immediate Leave (CLI)	41
Configuring MLD Snooping Queries (CLI)	42
Disabling MLD Listener Message Suppression (CLI)	43
Displaying MLD Snooping Information	44
Configuration Examples for Configuring MLD Snooping	45
Configuring a Static Multicast Group: Example	45
Configuring a Multicast Router Port: Example	45
Enabling MLD Immediate Leave: Example	46
Configuring MLD Snooping Queries: Example	46

CHAPTER 4
Configuring IPv6 ACL 47

Finding Feature Information	47
Information About Configuring IPv6 ACLs	47
Understanding IPv6 ACLs	48
Supported ACL Features	48
IPv6 ACL Limitations	49
Configuring IPv6 ACLs	49
Default IPv6 ACL Configuration	50
Interaction with Other Features and Switches	50
Creating IPv6 ACL	50
Applying an IPv6 ACL to an Interface	53
Displaying IPv6 ACLs	54
Configuration Examples for IPv6 ACL	55
Example: Creating IPv6 ACL	55
Example: Applying IPv6 ACLs	55
Example: Displaying IPv6 ACLs	56



Preface

- [Document Conventions](#), page vii
- [Related Documentation](#), page ix
- [Obtaining Documentation and Submitting a Service Request](#), page ix

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in bold font .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <i>courier font</i> .
Bold Courier font	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{x y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Tip

Means *the following information will help you solve a problem*.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

**Note**

Before installing or upgrading the switch, refer to the release notes.

- Catalyst 2960-X Switch, located at http://www.cisco.com/go/cat2960x_docs.
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at: http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Using the Command-Line Interface

This chapter contains the following topics:

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 6](#)

Information About Using the Command-Line Interface

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switchcontrollerdevice reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switchcontrollerdevice reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname **Switch**

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	SwitchControllerDevice>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	SwitchControllerDevice#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode. Use this mode to execute privilege EXEC commands for access points. These commands are not part of the running config of the controller, they are sent to the IOS config of the access point.
Global configuration	While in privileged EXEC mode, enter the configure command.	SwitchControllerDevice(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire switchcontrollerdevice. Use this mode to configure access point commands that are part of the running config of the controller.
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	SwitchControllerDevice(config-vlan)#		

Mode	Access Method	Prompt	Exit Method	About This Mode
			<p>To exit to global configuration mode, enter the exit command.</p> <p>To return to privileged EXEC mode, press Ctrl-Z or enter end.</p>	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switchcontrollerdevice startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	SwitchControllerDevice(config-if)#	<p>To exit to global configuration mode, enter exit.</p> <p>To return to privileged EXEC mode, press Ctrl-Z or enter end.</p>	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	SwitchControllerDevice(config-line)#	<p>To exit to global configuration mode, enter exit.</p> <p>To return to privileged EXEC mode, press Ctrl-Z or enter end.</p>	Use this mode to configure parameters for the terminal line.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

DETAILED STEPS

	Command or Action	Purpose
Step 1	help Example: SwitchControllerDevice# help	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i> Example: SwitchControllerDevice# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry <Tab></i> Example: SwitchControllerDevice# sh conf<tab> SwitchControllerDevice# show configuration	Completes a partial command name.
Step 4	? Example: SwitchControllerDevice> ?	Lists all commands available for a particular command mode.
Step 5	<i>command ?</i> Example: SwitchControllerDevice> show ?	Lists the associated keywords for a command.
Step 6	<i>command keyword ?</i> Example: SwitchControllerDevice(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the switchcontrollerdevice to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
SwitchControllerDevice# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switchcontrollerdevice.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
<code>% Ambiguous command: "show con"</code>	You did not enter enough characters for your switchcontrollerdevice to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.
<code>% Incomplete command.</code>	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
<code>% Invalid input detected at '^' marker.</code>	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the switchcontrollerdevice configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.



Note Only CLI or HTTP changes are logged.

How to Use the CLI to Configure Features

Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the switchcontrollerdevice records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

SUMMARY STEPS

1. **terminal history** [*size number-of-lines*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal history [<i>size number-of-lines</i>] Example: SwitchControllerDevice# terminal history size 200	Changes the number of command lines that the switchcontrollerdevice records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Ctrl-P or use the up arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	Ctrl-N or use the down arrow key	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

	Command or Action	Purpose
Step 3	show history Example: SwitchControllerDevice# show history	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal no history Example: SwitchControllerDevice# terminal no history	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenable it.

SUMMARY STEPS

1. **terminal editing**
2. **terminal no editing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal editing Example: SwitchControllerDevice# terminal editing	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
Step 2	terminal no editing Example: SwitchControllerDevice# terminal no editing	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.



Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 3: Editing Commands

Editing Commands	Description
Ctrl-B or use the left arrow key	Moves the cursor back one character.
Ctrl-F or use the right arrow key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Delete or Backspace key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.

Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.
Ctrl-V or Esc Q	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Return key	Scrolls down a line or screen on displays that are longer than the terminal screen can display. Note The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.
Space bar	Scrolls down one screen.
Ctrl-L or Ctrl-R	Redisplays the current command line if the switchcontrollerdevice suddenly sends a message to your screen.

Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return key**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>access-list</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 SwitchControllerDevice(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 SwitchControllerDevice(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq SwitchControllerDevice(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.</p>
Step 2	<p>Ctrl-A</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
Step 3	<p>Return key</p>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

SUMMARY STEPS

1. `{show | more} command | {begin | include | exclude} regular-expression`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>{show more} <i>command</i> {begin include exclude} <i>regular-expression</i></p> <p>Example: SwitchControllerDevice# show interfaces include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</p>	<p>Searches and filters the output.</p> <p>Expressions are case sensitive. For example, if you enter exclude output, the lines that contain output are not displayed, but the lines that contain output appear.</p>

Accessing the CLI on a Switch Stack

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser.

You manage the switch stack and the stack member interfaces through the active switchstack master. You cannot manage stack members on an individual switch basis. You can connect to the active switchstack master through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switchstack master. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.



Note

We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

To debug a specific stack member, you can start a CLI session from the stack master by using the **session stack-member-number** privileged EXEC command. The stack member number is appended to the system prompt. For example, *Switch-2#* is the prompt for stack member 2 where the system prompt for the stack master is *Switch*. Only the **show** and **debug** commands are available in a CLI session to a specific stack member. You can also use the **remote command stack-member-number LINE** privileged EXEC command on the stack master to enable debugging on a member switch without first starting a session.

Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switchcontrollerdevice console or connect a PC to the Ethernet management port and then power on the switchcontrollerdevice, as described in the hardware installation guide that shipped with your switchcontrollerdevice.

If your switchcontrollerdevice is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switchcontrollerdevice must first be configured for this type of access.

You can use one of these methods to establish a connection with the switchcontrollerdevice:

- Connect the switchcontrollerdevice console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switchcontrollerdevice hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switchcontrollerdevice must have network connectivity with the Telnet or SSH client, and the switchcontrollerdevice must have an enable secret password configured.
 - The switchcontrollerdevice supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
 - The switchcontrollerdevice supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



Configuring IPv6 Unicast Routing

- [Finding Feature Information, page 15](#)
- [Information About Configuring IPv6 Host Functions , page 15](#)
- [Configuration Examples for IPv6 Unicast Routing, page 28](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information About Configuring IPv6 Host Functions

This chapter describes how to configure IPv6 host functions on the Catalyst 2960, 2960-S, and 2960-C.

**Note**

To use IPv6 Host Functions, the switch must be running the LAN Base image.

For information about configuring IPv6 Multicast Listener Discovery (MLD) snooping, see *Configuring MLD Snooping*.

To enable dual stack environments (supporting both IPv4 and IPv6) on a Catalyst 2960 switch, you must configure the switch to use the a dual IPv4 and IPv6 switch database management (SDM) template. See the ["Dual IPv4 and IPv6 Protocol Stacks" section](#). This template is not required on Catalyst 2960-S switches.

**Note**

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS documentation referenced in the procedures.

Understanding IPv6

IPv4 users can move to IPv6 and receive services such as end-to-end security, quality of service (QoS), and globally unique addresses. The IPv6 address space reduces the need for private addresses and Network Address Translation (NAT) processing by border routers at network edges.

For information about how Cisco Systems implements IPv6, go to:

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

For information about IPv6 and other features in this chapter

- See the *Cisco IOS IPv6 Configuration Library*.
- Use the Search field on Cisco.com to locate the Cisco IOS software documentation. For example, if you want information about static routes, you can enter *Implementing Static Routes for IPv6* in the search field to learn about static routes.

IPv6 Addresses

The switch supports only IPv6 unicast addresses. It does not support site-local unicast addresses, or anycast addresses.

The IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons in the format: n:n:n:n:n:n:n:n. This is an example of an IPv6 address:

```
2031:0000:130F:0000:0000:09C0:080F:130B
```

For easier implementation, leading zeros in each field are optional. This is the same address without leading zeros:

```
2031:0:130F:0:0:9C0:80F:130B
```

You can also use two colons (::) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

```
2031:0:130F::09C0:080F:130B
```

For more information about IPv6 address formats, address types, and the IPv6 packet header, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

In the “Implementing Addressing and Basic Connectivity” chapter, these sections apply to the Catalyst 2960, 2960-S, 2960-C, or 2960-X switch:

In the “Information About Implementing Basic Connectivity for IPv6” chapter, these sections apply to the switch:

- IPv6 Address Formats
- IPv6 Address Type: Unicast
- IPv6 Address Type: Multicast
- IPv6 Address Output Display
- Simplified IPv6 Packet Header

Supported IPv6 Unicast Routing Features

These sections describe the IPv6 protocol features supported by the switch:

Support on the switch includes expanded address capability, header format simplification, improved support of extensions and options, and hardware parsing of the extension header. The switch supports hop-by-hop extension header packets, which are routed or bridged in software.

The switch provides IPv6 routing capability over Routing Information Protocol (RIP) for IPv6, and Open Shortest Path First (OSPF) Version 3 Protocol. It supports up to 16 equal-cost routes and can simultaneously forward IPv4 and IPv6 frames at line rate.

128-Bit Wide Unicast Addresses

The switch supports aggregatable global unicast addresses and link-local unicast addresses. It does not support site-local unicast addresses.

- Aggregatable global unicast addresses are IPv6 addresses from the aggregatable global unicast prefix. The address structure enables strict aggregation of routing prefixes and limits the number of routing table entries in the global routing table. These addresses are used on links that are aggregated through organizations and eventually to the Internet service provider.

These addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Addresses with a prefix of 2000::/3(001) through E000::/3(111) must have 64-bit interface identifiers in the extended unique identifier (EUI)-64 format.

- Link local unicast addresses can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the modified EUI format. Link-local addresses are used in the neighbor discovery protocol (NDP) and the stateless autoconfiguration process. Nodes on a local link use link-local addresses and do not require globally unique addresses to communicate. IPv6 routers do not forward packets with link-local source or destination addresses to other links.

For more information, see the section about IPv6 unicast addresses in the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

DNS for IPv6

IPv6 supports Domain Name System (DNS) record types in the DNS name-to-address and address-to-name lookup processes. The DNS AAAA resource record types support IPv6 addresses and are equivalent to an A address record in IPv4. The switch supports DNS resolution for IPv4 and IPv6.

ICMPv6

The Internet Control Message Protocol (ICMP) in IPv6 generates error messages, such as ICMP destination unreachable messages, to report errors during processing and other diagnostic functions. In IPv6, ICMP packets are also used in the neighbor discovery protocol and path MTU discovery.

Neighbor Discovery

The switch supports NDP for IPv6, a protocol running on top of ICMPv6, and static neighbor entries for IPv6 stations that do not support NDP. The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), to verify the reachability of the neighbor, and to keep track of neighboring routers.

The switch supports ICMPv6 redirect for routes with mask lengths less than 64 bits. ICMP redirect is not supported for host routes or for summarized routes with mask lengths greater than 64 bits.

Neighbor discovery throttling ensures that the switch CPU is not unnecessarily burdened while it is in the process of obtaining the next hop forwarding information to route an IPv6 packet. The switch drops any additional IPv6 packets whose next hop is the same neighbor that the switch is actively trying to resolve. This drop avoids further load on the CPU.

**Note**

First Hop Security in IPv6 is not supported on EtherChannels.

IPv6 Stateless Autoconfiguration and Duplicate Address Detection

The switch uses stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses. A host autonomously configures its own link-local address, and booting nodes send router solicitations to request router advertisements for configuring interfaces.

For more information about autoconfiguration and duplicate address detection, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

IPv6 Applications

The switch has IPv6 support for these applications:

- Ping, traceroute, and Telnet, and TFTP
- Secure Shell (SSH) over an IPv6 transport
- HTTP server access over IPv6 transport
- DNS resolver for AAAA over IPv4 transport
- Cisco Discovery Protocol (CDP) support for IPv6 addresses

For more information about managing these applications, see the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

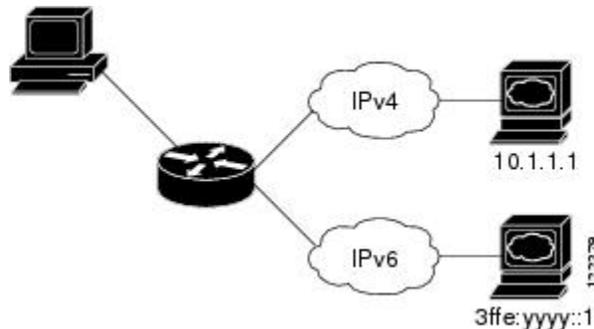
Dual IPv4 and IPv6 Protocol Stacks

On a Catalyst 2960-X switch, you must use the dual IPv4 and IPv6 template to allocate ternary content addressable memory (TCAM) usage to both IPv4 and IPv6 protocols.

You must use the dual IPv4 and IPv6 template to allocate hardware memory usage to both IPv4 and IPv6 protocols.

This figure shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.

Figure 1: Dual IPv4 and IPv6 Support on an Interface



Use the dual IPv4 and IPv6 switch database management (SDM) template to enable IPv6 routing dual stack environments (supporting both IPv4 and IPv6). For more information about the dual IPv4 and IPv6 SDM template, see *Configuring SDM Templates*.

The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments.

- If you try to configure IPv6 without first selecting a dual IPv4 and IPv6 template, a warning message appears.
- In IPv4-only environments, the switch routes IPv4 packets and applies IPv4 QoS and ACLs in hardware. IPv6 packets are not supported.
- In dual IPv4 and IPv6 environments, the switch applies IPv4 QoS and ACLs in hardware .
- The switch supports QoS for both IPv4 and IPv6 traffic.
- IPv6 QoS and ACLs are not supported.
- If you do not plan to use IPv6, do not use the dual stack template because this template results in less hardware memory capacity for each resource.

For more information about IPv4 and IPv6 protocol stacks, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

SNMP and Syslog Over IPv6

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

SNMP and syslog over IPv6 provide these features:

- Support for both IPv4 and IPv6
- IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host
- SNMP- and syslog-related MIBs to support IPv6 addressing
- Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

- Opens User Datagram Protocol (UDP) SNMP socket with default settings
- Provides a new transport mechanism called *SR_IPV6_TRANSPORT*
- Sends SNMP notifications over IPv6 transport
- Supports SNMP-named access lists for IPv6 transport
- Supports SNMP proxy forwarding using IPv6 transport
- Verifies SNMP Manager feature works with IPv6 transport

For information on SNMP over IPv6, including configuration procedures, see the “Managing Cisco IOS Applications over IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

For information about syslog over IPv6, including configuration procedures, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

HTTP(S) Over IPv6

The HTTP client sends requests to both IPv4 and IPv6 HTTP servers, which respond to requests from both IPv4 and IPv6 HTTP clients. URLs with literal IPv6 addresses must be specified in hexadecimal using 16-bit values between colons.

The accept socket call chooses an IPv4 or IPv6 address family. The accept socket is either an IPv4 or IPv6 socket. The listening socket continues to listen for both IPv4 and IPv6 signals that indicate a connection. The IPv6 listening socket is bound to an IPv6 wildcard address.

The underlying TCP/IP stack supports a dual-stack environment. HTTP relies on the TCP/IP stack and the sockets for processing network-layer interactions.

Basic network connectivity (**ping**) must exist between the client and the server hosts before HTTP connections can be made.

For more information, see the “Managing Cisco IOS Applications over IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

IPv6 and Switch Stacks

The switch supports IPv6 forwarding across the stack and IPv6 host functionality on the stack master. The stack master runs IPv6 host functionality and IPv6 applications.

While the new stack master is being elected and is resetting, the switch stack does not forward IPv6 packets. The stack MAC address changes, which also changes the IPv6 address. When you specify the stack IPv6 address with an extended unique identifier (EUI) by using the **ipv6 address ipv6-prefix/prefix length eui-64** interface configuration command, the address is based on the interface MAC address. See the "[Configuring IPv6 Addressing and Enabling IPv6 Host](#)" section.

If you configure the persistent MAC address feature on the stack and the stack master changes, the stack MAC address does not change for approximately 4 minutes. For more information, see the "Enabling Persistent MAC Address" section in "Managing Switch Stacks."

Default IPv6 Configuration

Table 4: Default IPv6 Configuration

Feature	Default Setting
SDM template	Advance desktop. Default is advanced template
IPv6 routing	Disabled globally and on all interfaces
CEFv6 or dCEFv6	Disabled (IPv4 CEF and dCEF are enabled by default) Note When IPv6 routing is enabled, CEFv6 and dCEF6 are automatically enabled.
IPv6 addresses	None configured

Configuring IPv6 Addressing and Enabling IPv6 Routing

This section describes how to assign IPv6 addresses to individual Layer 3 interfaces and to globally forward IPv6 traffic on the switch.

Before configuring IPv6 on the switch, consider these guidelines:

- Be sure to select a dual IPv4 and IPv6 SDM template.
- In the **ipv6 address** interface configuration command, you must enter the *ipv6-address* and *ipv6-prefix* variables with the address specified in hexadecimal using 16-bit values between colons. The *prefix-length* variable (preceded by a slash [/]) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

To forward IPv6 traffic on an interface, you must configure a global IPv6 address on that interface. Configuring an IPv6 address on an interface automatically configures a link-local address and activates IPv6 for the interface. The configured interface automatically joins these required multicast groups for that link:

- solicited-node multicast group FF02:0:0:0:0:1:ff00::/104 for each unicast address assigned to the interface (this address is used in the neighbor discovery process.)
- all-nodes link-local multicast group FF02::1
- all-routers link-local multicast group FF02::2

For more information about configuring IPv6 routing, see the “Implementing Addressing and Basic Connectivity for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

Beginning in privileged EXEC mode, follow these steps to assign an IPv6 address to a Layer 3 interface and enable IPv6 forwarding:

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>SwitchControllerDevice# configure terminal</pre>	Enters global configuration mode.
Step 2	<p>sdm prefer dual-ipv4-and-ipv6 {default}</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# sdm prefer dual-ipv4-and-ipv6 default</pre>	<p>Selects an SDM template that supports IPv4 and IPv6.</p> <ul style="list-style-type: none"> • default—Sets the switch to the default template to balance system resources.
Step 3	<p>end</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# end</pre>	Returns to privileged EXEC mode.
Step 4	<p>reload</p> <p>Example:</p> <pre>SwitchControllerDevice# reload</pre>	Reloads the operating system.
Step 5	<p>configure terminal</p> <p>Example:</p> <pre>SwitchControllerDevice# configure terminal</pre>	Enters global configuration mode after the switch reloads.
Step 6	<p>interface interface-id</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 7	<p>Use one of the following:</p> <ul style="list-style-type: none"> • ipv6 address ipv6-prefix/prefix length eui-64 • ipv6 address ipv6-address/prefix length • ipv6 address ipv6-address link-local • ipv6 enable 	<ul style="list-style-type: none"> • Specifies a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. This enables IPv6 processing on the interface. • Manually configures an IPv6 address on the interface. • Specifies a link-local address on the interface to be used instead of the link-local address that is automatically

	Command or Action	Purpose
	<p>Example:</p> <pre>SwitchControllerDevice(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64</pre> <pre>SwitchControllerDevice(config-if)# ipv6 address 2001:0DB8:c18:1::/64</pre> <pre>SwitchControllerDevice(config-if)# ipv6 address 2001:0DB8:c18:1:: link-local</pre> <pre>SwitchControllerDevice(config-if)# ipv6 enable</pre>	<p>configured when IPv6 is enabled on the interface. This command enables IPv6 processing on the interface.</p> <ul style="list-style-type: none"> Automatically configures an IPv6 link-local address on the interface, and enables the interface for IPv6 processing. The link-local address can only be used to communicate with nodes on the same link.
Step 8	<p>exit</p> <p>Example:</p> <pre>SwitchControllerDevice(config-if)# exit</pre>	Returns to global configuration mode.
Step 9	<p>end</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# end</pre>	Returns to privileged EXEC mode.
Step 10	<p>show ipv6 interface <i>interface-id</i></p> <p>Example:</p> <pre>SwitchControllerDevice# show ipv6 interface gigabitethernet 1/0/1</pre>	Verifies your entries.
Step 11	<p>copy running-config startup-config</p> <p>Example:</p> <pre>SwitchControllerDevice# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring IPv6 ICMP Rate Limiting (CLI)

ICMP rate limiting is enabled by default with a default interval between error messages of 100 milliseconds and a bucket size (maximum number of tokens to be stored in a bucket) of 10.

Beginning in privileged EXEC mode, follow these steps to change the ICMP rate-limiting parameters:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	ipv6 icmp error-interval interval [bucketsize] Example: SwitchControllerDevice(config)# ipv6 icmp error-interval 50 20	Configures the interval and bucket size for IPv6 ICMP error messages: <ul style="list-style-type: none"> • <i>interval</i>—The interval (in milliseconds) between tokens being added to the bucket. The range is from 0 to 2147483647 milliseconds. • <i>bucketsize</i>—(Optional) The maximum number of tokens stored in the bucket. The range is from 1 to 200.
Step 3	end Example: SwitchControllerDevice(config)# end	Returns to privileged EXEC mode.
Step 4	show ipv6 interface [interface-id] Example: SwitchControllerDevice# show ipv6 interface gigabitethernet 1/0/1	Verifies your entries.
Step 5	copy running-config startup-config Example: SwitchControllerDevice# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Static Routing for IPv6 (CLI)

Before configuring a static IPv6 route, you must enable routing by using the **ip routing** global configuration command, enable the forwarding of IPv6 packets by using the **ipv6 unicast-routing** global configuration command, and enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.

For more information about configuring static IPv6 routing, see the “Implementing Static Routes for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>SwitchControllerDevice# configure terminal</pre>	Enters global configuration mode.
Step 2	<p>ipv6 route <i>ipv6-prefix/prefix length</i> <i>{ipv6-address interface-id [ipv6-address]}</i> <i>[administrative distance]</i></p> <p>Example:</p> <pre>SwitchControllerDevice(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130</pre>	<p>Configures a static IPv6 route.</p> <ul style="list-style-type: none"> • <i>ipv6-prefix</i>—The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured. • <i>/prefix length</i>—The length of the IPv6 prefix. A decimal value that shows 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. • <i>ipv6-address</i>—The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. The address must be in the form documented in RFC 2373, specified in hexadecimal using 16-bit values between colons. • <i>interface-id</i>—Specifies direct static routes from point-to-point and broadcast interfaces. With point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. With broadcast interfaces, you should always specify the IPv6 address of the next hop, or ensure that the specified prefix is assigned to the link, specifying a link-local address as the next hop. You can optionally specify the IPv6 address of the next hop to which packets are sent. <p>Note You must specify an <i>interface-id</i> when using a link-local address as the next hop (the link-local next hop must also be an adjacent router).</p> <ul style="list-style-type: none"> • <i>administrative distance</i>—(Optional) An administrative distance. The range is 1 to 254; the default value is 1, which gives static routes precedence over any other type of route except connected routes. To configure a floating static route, use an administrative distance greater than that of the dynamic routing protocol.
Step 3	<p>end</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# end</pre>	Returns to privileged EXEC mode.
Step 4	Use one of the following:	Verifies your entries by displaying the contents of the IPv6 routing table.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • show ipv6 static [<i>ipv6-address</i> <i>ipv6-prefix/prefix length</i>] [interface <i>interface-id</i>] [detail][recursive] [detail] • show ipv6 route static [<i>updated</i>] <p>Example: SwitchControllerDevice# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1</p> <p>OR</p> SwitchControllerDevice# show ipv6 route static	<ul style="list-style-type: none"> • interface <i>interface-id</i>—(Optional) Displays only those static routes with the specified interface as an egress interface. • recursive—(Optional) Displays only recursive static routes. The recursive keyword is mutually exclusive with the interface keyword, but it can be used with or without the IPv6 prefix included in the command syntax. • detail—(Optional) Displays this additional information: <ul style="list-style-type: none"> ◦ For valid recursive routes, the output path set, and maximum resolution depth. ◦ For invalid routes, the reason why the route is not valid.
Step 5	copy running-config startup-config <p>Example: SwitchControllerDevice# copy running-config startup-config</p>	(Optional) Saves your entries in the configuration file.

Displaying IPv6

For complete syntax and usage information on these commands, see the Cisco IOS command reference publications.

Table 5: Command for Monitoring IPv6

Command	Purpose
show ipv6 access-list	Displays a summary of access lists.
show ipv6 cef	Displays Cisco Express Forwarding for IPv6.
show ipv6 interface <i>interface-id</i>	Displays IPv6 interface status and configuration.
show ipv6 mtu	Displays IPv6 MTU per destination cache.
show ipv6 neighbors	Displays IPv6 neighbor cache entries.
show ipv6 ospf	Displays IPv6 OSPF information.
show ipv6 prefix-list	Displays a list of IPv6 prefix lists.

Command	Purpose
show ipv6 protocols	Displays a list of IPv6 routing protocols on the switch.
show ipv6 rip	Displays IPv6 RIP routing protocol status.
show ipv6 rip	Displays IPv6 RIP routing protocol status.
show ipv6 route	Displays IPv6 route table entries.
show ipv6 routers	Displays the local IPv6 routers.
show ipv6 static	Displays IPv6 static routes.
show ipv6 traffic	Displays IPv6 traffic statistics.

Table 6: Command for Displaying EIGRP IPv6 Information

Command	Purpose
show ipv6 eigrp [<i>as-number</i>] <i>interface</i>	Displays information about interfaces configured for EIGRP IPv6.
show ipv6 eigrp [<i>as-number</i>] <i>neighbor</i>	Displays the neighbors discovered by EIGRP IPv6.
show ipv6 interface [<i>as-number</i>] <i>traffic</i>	Displays the number of EIGRP IPv6 packets sent and received.
show ipv6 eigrptopology [<i>as-number</i> <i>ipv6-address</i>] [active all-links detail-links pending summary zero-successors Base]	Displays EIGRP entries in the IPv6 topology table.

Table 7: Command for Displaying EIGRP IPv6 Information

Command	Purpose
show ipv6 eigrptopology [<i>as-number</i> <i>ipv6-address</i>] [active all-links detail-links pending summary zero-successors]	Displays EIGRP entries in the IPv6 topology table.

Configuration Examples for IPv6 Unicast Routing

Configuring IPv6 Addressing and Enabling IPv6 Routing: Example

This example shows how to enable IPv6 with both a link-local address and a global address based on the IPv6 prefix 2001:0DB8:c18:1::/64. The EUI-64 interface ID is used in the low-order 64 bits of both addresses. Output from the **show ipv6 interface EXEC** command is included to show how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
SwitchControllerDevice(config)# ipv6 unicast-routing
SwitchControllerDevice(config)# interface gigabitethernet1/0/11
SwitchControllerDevice(config-if)# no switchport
SwitchControllerDevice(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
SwitchControllerDevice(config-if)# end
SwitchControllerDevice# show ipv6 interface gigabitethernet1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FE02::1
    FE02::2
    FE02::1:FE2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  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
  Hosts use stateless autoconfig for addresses.
```

Configuring IPv6 ICMP Rate Limiting: Example

This example shows how to configure an IPv6 ICMP error message interval of 50 milliseconds and a bucket size of 20 tokens.

```
SwitchControllerDevice(config)#ipv6 icmp error-interval 50 20
```

Configuring Static Routing for IPv6: Example

This example shows how to configure a floating static route to an interface with an administrative distance of 130:

```
SwitchControllerDevice(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

Displaying IPv6: Example

This is an example of the output from the **show ipv6 interface** privileged EXEC command:

```
SwitchControllerDevice# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
  3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
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
<output truncated>
```




Configuring MLD Snooping

This module contains details of configuring MLD snooping

- [Finding Feature Information, page 31](#)
- [Information About Configuring IPv6 MLD Snooping, page 31](#)
- [How to Configure IPv6 MLD Snooping, page 36](#)
- [Displaying MLD Snooping Information, page 44](#)
- [Configuration Examples for Configuring MLD Snooping, page 45](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information About Configuring IPv6 MLD Snooping

**Note**

To use IPv6 MLD Snooping, the switch must be running the LAN Base image.

You can use Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP Version 6 (IPv6) multicast data to clients and routers in a switched network on the switch. Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.

**Note**

Stacking is supported only on Catalyst 2960-X switches running the LAN base image.



Note To use IPv6 on a Catalyst 2960-X switch, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.



Note To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch.
On switches running the LAN Base feature set, the routing template is not supported.



Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

Understanding MLD Snooping

In IP Version 4 (IPv4), Layer 2 switches can use Internet Group Management Protocol (IGMP) snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on the links that are directly attached to the routers and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD Version 1 (MLDv1) is equivalent to IGMPv2, and MLD Version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol Version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch supports two versions of MLD snooping:

- MLDv1 snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination multicast addresses.
- MLDv2 basic snooping (MBSS) uses MLDv2 control packets to set up traffic forwarding based on IPv6 destination multicast addresses.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast addresses.



Note The switch does not support MLDv2 enhanced snooping, which sets up IPv6 source and destination multicast address-based forwarding.

MLD snooping can be enabled or disabled globally or per VLAN. When MLD snooping is enabled, a per-VLAN IPv6 multicast address table is constructed in software and hardware. The switch then performs IPv6 multicast-address based bridging in hardware.

According to IPv6 multicast standards, the switch derives the MAC multicast address by performing a logical-OR of the four low-order octets of the switch MAC address with the MAC address of 33:33:00:00:00:00.

For example, the IPv6 MAC address of FF02:DEAD:BEEF:1:3 maps to the Ethernet MAC address of 33:33:00:01:00:03.

A multicast packet is unmatched when the destination IPv6 address does not match the destination MAC address. The switch forwards the unmatched packet in hardware based on the MAC address table. If the destination MAC address is not in the MAC address table, the switch floods the packet to all ports in the same VLAN as the receiving port.

MLD Messages

MLDv1 supports three types of messages:

- Listener Queries are the equivalent of IGMPv2 queries and are either General Queries or Multicast-Address-Specific Queries (MASQs).
- Multicast Listener Reports are the equivalent of IGMPv2 reports
- Multicast Listener Done messages are the equivalent of IGMPv2 leave messages.

MLDv2 supports MLDv2 queries and reports, as well as MLDv1 Report and Done messages.

Message timers and state transitions resulting from messages being sent or received are the same as those of IGMPv2 messages. MLD messages that do not have valid link-local IPv6 source addresses are ignored by MLD routers and switches.

MLD Queries

The switch sends out MLD queries, constructs an IPv6 multicast address database, and generates MLD group-specific and MLD group-and-source-specific queries in response to MLD Done messages. The switch also supports report suppression, report proxying, Immediate-Leave functionality, and static IPv6 multicast group address configuration.

When MLD snooping is disabled, all MLD queries are flooded in the ingress VLAN.

When MLD snooping is enabled, received MLD queries are flooded in the ingress VLAN, and a copy of the query is sent to the CPU for processing. From the received query, MLD snooping builds the IPv6 multicast address database. It detects multicast router ports, maintains timers, sets report response time, learns the querier IP source address for the VLAN, learns the querier port in the VLAN, and maintains multicast-address aging.



Note

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the Catalyst 2960, 2960-S, 2960-C, or 2960-X switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

When a group exists in the MLD snooping database, the switch responds to a group-specific query by sending an MLDv1 report. When the group is unknown, the group-specific query is flooded to the ingress VLAN.

When a host wants to leave a multicast group, it can send out an MLD Done message (equivalent to IGMP Leave message). When the switch receives an MLDv1 Done message, if Immediate-Leave is not enabled, the switch sends an MASQ to the port from which the message was received to determine if other devices connected to the port should remain in the multicast group.

Multicast Client Aging Robustness

You can configure port membership removal from addresses based on the number of queries. A port is removed from membership to an address only when there are no reports to the address on the port for the configured number of queries. The default number is 2.

Multicast Router Discovery

Like IGMP snooping, MLD snooping performs multicast router discovery, with these characteristics:

- Ports configured by a user never age out.
- Dynamic port learning results from MLDv1 snooping queries and IPv6 PIMv2 packets.
- If there are multiple routers on the same Layer 2 interface, MLD snooping tracks a single multicast router on the port (the router that most recently sent a router control packet).
- Dynamic multicast router port aging is based on a default timer of 5 minutes; the multicast router is deleted from the router port list if no control packet is received on the port for 5 minutes.
- IPv6 multicast router discovery only takes place when MLD snooping is enabled on the switch.
- Received IPv6 multicast router control packets are always flooded to the ingress VLAN, whether or not MLD snooping is enabled on the switch.
- After the discovery of the first IPv6 multicast router port, unknown IPv6 multicast data is forwarded only to the discovered router ports (before that time, all IPv6 multicast data is flooded to the ingress VLAN).

MLD Reports

The processing of MLDv1 join messages is essentially the same as with IGMPv2. When no IPv6 multicast routers are detected in a VLAN, reports are not processed or forwarded from the switch. When IPv6 multicast routers are detected and an MLDv1 report is received, an IPv6 multicast group address is entered in the VLAN MLD database. Then all IPv6 multicast traffic to the group within the VLAN is forwarded using this address. When MLD snooping is disabled, reports are flooded in the ingress VLAN.

When MLD snooping is enabled, MLD report suppression, called listener message suppression, is automatically enabled. With report suppression, the switch forwards the first MLDv1 report received by a group to IPv6 multicast routers; subsequent reports for the group are not sent to the routers. When MLD snooping is disabled, report suppression is disabled, and all MLDv1 reports are flooded to the ingress VLAN.

The switch also supports MLDv1 proxy reporting. When an MLDv1 MASQ is received, the switch responds with MLDv1 reports for the address on which the query arrived if the group exists in the switch on another port and if the port on which the query arrived is not the last member port for the address.

MLD Done Messages and Immediate-Leave

When the Immediate-Leave feature is enabled and a host sends an MLDv1 Done message (equivalent to an IGMP leave message), the port on which the Done message was received is immediately deleted from the group. You enable Immediate-Leave on VLANs and (as with IGMP snooping), you should only use the feature on VLANs where a single host is connected to the port. If the port was the last member of a group, the group is also deleted, and the leave information is forwarded to the detected IPv6 multicast routers.

When Immediate Leave is not enabled in a VLAN (which would be the case when there are multiple clients for a group on the same port) and a Done message is received on a port, an MASQ is generated on that port. The user can control when a port membership is removed for an existing address in terms of the number of MASQs. A port is removed from membership to an address when there are no MLDv1 reports to the address on the port for the configured number of queries.

The number of MASQs generated is configured by using the **ipv6 mld snooping last-listener-query count** global configuration command. The default number is 2.

The MASQ is sent to the IPv6 multicast address for which the Done message was sent. If there are no reports sent to the IPv6 multicast address specified in the MASQ during the switch maximum response time, the port on which the MASQ was sent is deleted from the IPv6 multicast address database. The maximum response time is the time configured by using the **ipv6 mld snooping last-listener-query-interval** global configuration command. If the deleted port is the last member of the multicast address, the multicast address is also deleted, and the switch sends the address leave information to all detected multicast routers.

When Immediate Leave is not enabled and a port receives an MLD Done message, the switch generates MASQs on the port and sends them to the IPv6 multicast address for which the Done message was sent. You can optionally configure the number of MASQs that are sent and the length of time the switch waits for a response before deleting the port from the multicast group.

When you enable MLDv1 Immediate Leave, the switch immediately removes a port from a multicast group when it detects an MLD Done message on that port. You should only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN. When there are multiple clients for a multicast group on the same port, you should not enable Immediate-Leave in a VLAN.

Topology Change Notification Processing

When topology change notification (TCN) solicitation is enabled by using the **ipv6 mld snooping tcn query solicit** global configuration command, MLDv1 snooping sets the VLAN to flood all IPv6 multicast traffic with a configured number of MLDv1 queries before it begins sending multicast data only to selected ports. You set this value by using the **ipv6 mld snooping tcn flood query count** global configuration command. The default is to send two queries. The switch also generates MLDv1 global Done messages with valid link-local IPv6 source addresses when the switch becomes the STP root in the VLAN or when it is configured by the user. This is same as done in IGMP snooping.

MLD Snooping in Switch Stacks

The MLD IPv6 group address databases are maintained on all switches in the stack, regardless of which switch learns of an IPv6 multicast group. Report suppression and proxy reporting are done stack-wide. During the maximum response time, only one received report for a group is forwarded to the multicast routers, regardless of which switch the report arrives on.

The election of a new stack master does not affect the learning or bridging of IPv6 multicast data; bridging of IPv6 multicast data does not stop during a stack master re-election. When a new switch is added to the stack, it synchronizes the learned IPv6 multicast information from the stack master. Until the synchronization is complete, data ingress on the newly added switch is treated as unknown multicast data.

How to Configure IPv6 MLD Snooping

Default MLD Snooping Configuration

Table 8: Default MLD Snooping Configuration

Feature	Default Setting
MLD snooping (Global)	Disabled.
MLD snooping (per VLAN)	Enabled. MLD snooping must be globally enabled for VLAN MLD snooping to take place.
IPv6 Multicast addresses	None configured.
IPv6 Multicast router ports	None configured.
MLD snooping Immediate Leave	Disabled.
MLD snooping robustness variable	Global: 2; Per VLAN: 0. Note The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.
Last listener query count	Global: 2; Per VLAN: 0. Note The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.
Last listener query interval	Global: 1000 (1 second); VLAN: 0. Note The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global interval.
TCN query solicit	Disabled.
TCN query count	2.
MLD listener suppression	Disabled. Enabled.

MLD Snooping Configuration Guidelines

When configuring MLD snooping, consider these guidelines:

- You can configure MLD snooping characteristics at any time, but you must globally enable MLD snooping by using the **ipv6 mld snooping** global configuration command for the configuration to take effect.

- When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.
- MLD snooping and IGMP snooping act independently of each other. You can enable both features at the same time on the switch.
- The maximum number of multicast entries allowed on the switch or switch stack is determined by the configured SDM template.
- The maximum number of address entries allowed for the switch or switch stack is 1000.
- The maximum number of address entries allowed for the switch or switch stack is 4000.

Enabling or Disabling MLD Snooping on the Switch (CLI)

By default, IPv6 MLD snooping is globally disabled on the switch and enabled on all VLANs. When MLD snooping is globally disabled, it is also disabled on all VLANs. When you globally enable MLD snooping, the VLAN configuration overrides the global configuration. That is, MLD snooping is enabled only on VLAN interfaces in the default state (enabled).

You can enable and disable MLD snooping on a per-VLAN basis or for a range of VLANs, but if you globally disable MLD snooping, it is disabled in all VLANs. If global snooping is enabled, you can enable or disable VLAN snooping.

Beginning in privileged EXEC mode, follow these steps to globally enable MLD snooping on the switch:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	ipv6 mld snooping Example: SwitchControllerDevice(config)# ipv6 mld snooping	Enables MLD snooping on the switch.
Step 3	end Example: SwitchControllerDevice(config)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 4	copy running-config startup-config Example: <pre>SwitchControllerDevice(config)# copy running-config startup-config</pre>	(Optional) Save your entries in the configuration file.
Step 5	reload Example: <pre>SwitchControllerDevice(config)# reload</pre>	Reload the operating system.

Enabling or Disabling MLD Snooping on a VLAN (CLI)



Note

When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the Catalyst 3750-E or 3560-E Catalyst 3750-X or 3560-X switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

Beginning in privileged EXEC mode, follow these steps to enable MLD snooping on a VLAN.

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>SwitchControllerDevice# configure terminal</pre>	Enters global configuration mode.
Step 2	ipv6 mld snooping Example: <pre>SwitchControllerDevice(config)# ipv6 mld snooping</pre>	Enables MLD snooping on the switch.

	Command or Action	Purpose
Step 3	ipv6 mld snooping vlan <i>vlan-id</i> Example: SwitchControllerDevice(config)# ipv6 mld snooping vlan 1	Enables MLD snooping on the VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. Note MLD snooping must be globally enabled for VLAN snooping to be enabled.
Step 4	end Example: SwitchControllerDevice(config)# ipv6 mld snooping vlan 1	Returns to privileged EXEC mode.

Configuring a Static Multicast Group (CLI)

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure an IPv6 multicast address and member ports for a VLAN.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode
Step 2	ipv6 mld snooping vlan <i>vlan-id</i> static <i>ipv6_multicast_address</i> interface <i>interface-id</i> Example: SwitchControllerDevice(config)# ipv6 mld snooping vlan 1 static FF12::3 interface gigabitethernet 1/0/1	Configures a multicast group with a Layer 2 port as a member of a multicast group: <ul style="list-style-type: none"> • <i>vlan-id</i> is the multicast group VLAN ID. The VLAN ID range is 1 to 1001 and 1006 to 4094. • <i>ipv6_multicast_address</i> is the 128-bit group IPv6 address. The address must be in the form specified in RFC 2373. • <i>interface-id</i> is the member port. It can be a physical interface or a port channel (1 to 48).

	Command or Action	Purpose
Step 3	end Example: SwitchControllerDevice(config)# end	Returns to privileged EXEC mode.
Step 4	Use one of the following: <ul style="list-style-type: none"> • show ipv6 mld snooping address • show ipv6 mld snooping address vlan <i>vlan-id</i> Example: SwitchControllerDevice# show ipv6 mld snooping address OR SwitchControllerDevice# show ipv6 mld snooping vlan 1	Verifies the static member port and the IPv6 address.

Configuring a Multicast Router Port (CLI)



Note Static connections to multicast routers are supported only on switch ports.

Beginning in privileged EXEC mode, follow these steps to add a multicast router port to a VLAN:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> Example: SwitchControllerDevice(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 1/0/2	Specifies the multicast router VLAN ID, and specify the interface to the multicast router. <ul style="list-style-type: none"> • The VLAN ID range is 1 to 1001 and 1006 to 4094. • The interface can be a physical interface or a port channel. The port-channel range is 1 to 48.

	Command or Action	Purpose
Step 3	end Example: SwitchControllerDevice(config)# end	Returns to privileged EXEC mode.
Step 4	show ipv6 mld snooping mrouter [vlan <i>vlan-id</i>] Example: SwitchControllerDevice# show ipv6 mld snooping mrouter vlan 1	Verifies that IPv6 MLD snooping is enabled on the VLAN interface.

Enabling MLD Immediate Leave (CLI)

Beginning in privileged EXEC mode, follow these steps to enable MLDv1 Immediate Leave:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	ipv6 mld snooping vlan <i>vlan-id</i> immediate-leave Example: SwitchControllerDevice(config)# ipv6 mld snooping vlan 1 immediate-leave	Enables MLD Immediate Leave on the VLAN interface.
Step 3	end Example: SwitchControllerDevice(config)# end	Returns to privileged EXEC mode.
Step 4	show ipv6 mld snooping vlan <i>vlan-id</i> Example: SwitchControllerDevice# show ipv6 mld snooping vlan 1	Verifies that Immediate Leave is enabled on the VLAN interface.

Configuring MLD Snooping Queries (CLI)

Beginning in privileged EXEC mode, follow these steps to configure MLD snooping query characteristics for the switch or for a VLAN:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	ipv6 mld snooping robustness-variable <i>value</i> Example: SwitchControllerDevice (config)# ipv6 mld snooping robustness-variable 3	(Optional) Sets the number of queries that are sent before switch will deletes a listener (port) that does not respond to a general query. The range is 1 to 3; the default is 2.
Step 3	ipv6 mld snooping vlan <i>vlan-id</i> robustness-variable <i>value</i> Example: SwitchControllerDevice (config)# ipv6 mld snooping vlan 1 robustness-variable 3	(Optional) Sets the robustness variable on a VLAN basis, which determines the number of general queries that MLD snooping sends before aging out a multicast address when there is no MLD report response. The range is 1 to 3; the default is 0. When set to 0, the number used is the global robustness variable value.
Step 4	ipv6 mld snooping last-listener-query-count <i>count</i> Example: SwitchControllerDevice (config)# ipv6 mld snooping last-listener-query-count 7	(Optional) Sets the number of MASQs that the switch sends before aging out an MLD client. The range is 1 to 7; the default is 2. The queries are sent 1 second apart.
Step 5	ipv6 mld snooping vlan <i>vlan-id</i> last-listener-query-count <i>count</i> Example: SwitchControllerDevice (config)# ipv6 mld snooping vlan 1 last-listener-query-count 7	(Optional) Sets the last-listener query count on a VLAN basis. This value overrides the value configured globally. The range is 1 to 7; the default is 0. When set to 0, the global count value is used. Queries are sent 1 second apart.
Step 6	ipv6 mld snooping last-listener-query-interval <i>interval</i> Example: SwitchControllerDevice (config)# ipv6 mld snooping last-listener-query-interval 2000	(Optional) Sets the maximum response time that the switch waits after sending out a MASQ before deleting a port from the multicast group. The range is 100 to 32,768 thousands of a second. The default is 1000 (1 second).
Step 7	ipv6 mld snooping vlan <i>vlan-id</i> last-listener-query-interval <i>interval</i>	(Optional) Sets the last-listener query interval on a VLAN basis. This value overrides the value configured globally. The range is

	Command or Action	Purpose
	Example: <pre>SwitchControllerDevice(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 2000</pre>	0 to 32,768 thousands of a second. The default is 0. When set to 0, the global last-listener query interval is used.
Step 8	ipv6 mld snooping tcn query solicit Example: <pre>SwitchControllerDevice(config)# ipv6 mld snooping tcn query solicit</pre>	(Optional) Enables topology change notification (TCN) solicitation, which means that VLANs flood all IPv6 multicast traffic for the configured number of queries before sending multicast data to only those ports requesting to receive it. The default is for TCN to be disabled.
Step 9	ipv6 mld snooping tcn flood query count <i>count</i> Example: <pre>SwitchControllerDevice(config)# ipv6 mld snooping tcn flood query count 5</pre>	(Optional) When TCN is enabled, specifies the number of TCN queries to be sent. The range is from 1 to 10; the default is 2.
Step 10	end	Returns to privileged EXEC mode.
Step 11	show ipv6 mld snooping querier [vlan <i>vlan-id</i>] Example: <pre>SwitchControllerDevice(config)# show ipv6 mld snooping querier vlan 1</pre>	(Optional) Verifies that the MLD snooping querier information for the switch or for the VLAN.

Disabling MLD Listener Message Suppression (CLI)

MLD snooping listener message suppression is enabled by default. When it is enabled, the switch forwards only one MLD report per multicast router query. When message suppression is disabled, multiple MLD reports could be forwarded to the multicast routers.

Beginning in privileged EXEC mode, follow these steps to disable MLD listener message suppression:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>SwitchControllerDevice# configure terminal</pre>	Enter global configuration mode.

	Command or Action	Purpose
Step 2	no ipv6 mld snooping listener-message-suppression Example: SwitchControllerDevice(config)# no ipv6 mld snooping listener-message-suppression	Disable MLD message suppression.
Step 3	end Example: SwitchControllerDevice(config)# end	Return to privileged EXEC mode.
Step 4	show ipv6 mld snooping Example: SwitchControllerDevice# show ipv6 mld snooping	Verify that IPv6 MLD snooping report suppression is disabled.

Displaying MLD Snooping Information

You can display MLD snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display IPv6 group address multicast entries for a VLAN configured for MLD snooping.

Table 9: Commands for Displaying MLD Snooping Information

Command	Purpose
show ipv6 mld snooping [vlan <i>vlan-id</i>]	Displays the MLD snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter vlan <i>vlan-id</i> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
show ipv6 mld snooping mrouter [vlan <i>vlan-id</i>]	Displays information on dynamically learned and manually configured multicast router interfaces. When you enable MLD snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces. (Optional) Enters vlan <i>vlan-id</i> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.

Command	Purpose
show ipv6 mld snooping querier [vlan <i>vlan-id</i>]	Displays information about the IPv6 address and incoming port for the most-recently received MLD query messages in the VLAN. (Optional) Enters vlan <i>vlan-id</i> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
show ipv6 mld snooping address [vlan <i>vlan-id</i>] [count dynamic user]	Displays all IPv6 multicast address information or specific IPv6 multicast address information for the switch or a VLAN. <ul style="list-style-type: none"> • Enters count to show the group count on the switch or in a VLAN. • Enters dynamic to display MLD snooping learned group information for the switch or for a VLAN. • Enters user to display MLD snooping user-configured group information for the switch or for a VLAN.
show ipv6 mld snooping address vlan <i>vlan-id</i> [<i>ipv6-multicast-address</i>]	Displays MLD snooping for the specified VLAN and IPv6 multicast address.

Configuration Examples for Configuring MLD Snooping

Configuring a Static Multicast Group: Example

This example shows how to statically configure an IPv6 multicast group:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ipv6 mld snooping vlan 2 static FF12::3 interface
gigabitethernet
    1/
    1/0/1
SwitchControllerDevice(config)# end
```

Configuring a Multicast Router Port: Example

This example shows how to add a multicast router port to VLAN 200:

```
SwitchControllerDevice# configure terminal
SwitchControllerDevice(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet
```

```
1/  
0/2  
SwitchControllerDevice(config)# exit
```

Enabling MLD Immediate Leave: Example

This example shows how to enable MLD Immediate Leave on VLAN 130:

```
SwitchControllerDevice# configure terminal  
SwitchControllerDevice(config)# ipv6 mld snooping vlan 130 immediate-leave  
SwitchControllerDevice(config)# exit
```

Configuring MLD Snooping Queries: Example

This example shows how to set the MLD snooping global robustness variable to 3:

```
SwitchControllerDevice# configure terminal  
SwitchControllerDevice(config)# ipv6 mld snooping robustness-variable 3  
SwitchControllerDevice(config)# exit
```

This example shows how to set the MLD snooping last-listener query count for a VLAN to 3:

```
SwitchControllerDevice# configure terminal  
SwitchControllerDevice(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3  
SwitchControllerDevice(config)# exit
```

This example shows how to set the MLD snooping last-listener query interval (maximum response time) to 2000 (2 seconds):

```
SwitchControllerDevice# configure terminal  
SwitchControllerDevice(config)# ipv6 mld snooping last-listener-query-interval 2000  
SwitchControllerDevice(config)# exit
```



Configuring IPv6 ACL

- [Finding Feature Information, page 47](#)
- [Information About Configuring IPv6 ACLs, page 47](#)
- [Configuring IPv6 ACLs, page 49](#)
- [Configuration Examples for IPv6 ACL, page 55](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Information About Configuring IPv6 ACLs

You can filter IP version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP version 4 (IPv4) named ACLs. You can also create and apply input router ACLs to filter Layer 3 management traffic.



Note

To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the **sdm prefer {default | dual-ipv4-and-ipv6}** global configuration command.



Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

Understanding IPv6 ACLs

A switch image supports two types of IPv6 ACLs:

- IPv6 router ACLs - Supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels. Applied to only IPv6 packets that are routed.
- IPv6 port ACLs - Supported on inbound traffic on Layer 2 interfaces only. Applied to all IPv6 packets entering the interface.

**Note**

If you configure unsupported IPv6 ACLs, an error message appears and the configuration does not take affect.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface.

As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs:

- When an input router ACL and input port ACL exist in an SVI, packets received on ports to which a port ACL is applied are filtered by the port ACL. Routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IPv6 packets are filtered by the router ACL. Other packets are not filtered.

**Note**

If any port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

Supported ACL Features

IPv6 ACLs on the switch have these characteristics:

- Fragmented frames (the fragments keyword as in IPv4) are supported.
- The same statistics supported in IPv4 are supported for IPv6 ACLs.
- If the switch runs out of TCAM space, packets associated with the ACL label are forwarded to the CPU, and the ACLs are applied in software.
- Routed or bridged packets with hop-by-hop options have IPv6 ACLs applied in software.
- Logging is supported for router ACLs, but not for port ACLs.
- The switch supports IPv6 address-matching for a full range of prefix lengths.

IPv6 ACL Limitations

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:

- IPv6 source and destination addresses-ACL matching is supported only on prefixes from /0 to /64 and host addresses (/128) that are in the extended universal identifier (EUI)-64 format. The switch supports only these host addresses with no loss of information:
 - aggregatable global unicast addresses
 - link local addresses
- The switch does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.
- The switch does not support reflexive ACLs (the **reflect** keyword).
- This release supports only port ACLs and router ACLs for IPv6; it does not support VLAN ACLs (VLAN maps).
- The switch does not apply MAC-based ACLs on IPv6 frames.
- You cannot apply IPv6 port ACLs to Layer 2 EtherChannels.
- The switch does not support output port ACLs.
- Output router ACLs and input port ACLs for IPv6 are supported only on . Switches support only control plane (incoming) IPv6 ACLs.
- When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

Configuring IPv6 ACLs

Before configuring IPv6 ACLs, you must select one of the dual IPv4 and IPv6 SDM templates.

To filter IPv6 traffic, you perform these steps:

DETAILED STEPS

	Command or Action	Purpose
Step 1	Create an IPv6 ACL, and enter IPv6 access list configuration mode.	
Step 2	Configure the IPv6 ACL to block (deny) or pass (permit) traffic.	

	Command or Action	Purpose
Step 3	Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.	

Default IPv6 ACL Configuration

There are no IPv6 ACLs configured or applied.

Interaction with Other Features and Switches

- If an IPv6 router ACL is configured to deny a packet, the packet is not routed. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch or switch stack, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, for any additional configured ACLs, packets are dropped to the CPU, and the ACLs are applied in software. When the hardware is full a message is printed to the console indicating the ACL has been unloaded and the packets will be dropped on the interface.



Note Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be dropped on the interface.

Creating IPv6 ACL

Beginning in privileged EXEC mode, follow these steps to create an IPv6 ACL:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	ipv6access-list <i>access-list-name</i> Example: ipv6 access-list access-list-name	Define an IPv6 access list name, and enter IPv6 access-list configuration mode.
Step 3	{deny permit} protocol Example: <pre>{deny permit} protocol {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]][destination-ipv6-prefix/prefix-length any host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]</pre>	<p>Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions:</p> <ul style="list-style-type: none"> • For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number. • The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). • Enter any as an abbreviation for the IPv6 prefix ::/0. • For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. • (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. <p>If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6- prefix/prefix-length argument, it must match the destination port.</p> <ul style="list-style-type: none"> • (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP. • (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6. • (Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs. • (Optional) Enter routing to specify that IPv6 packets be routed. • (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295 • (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.
Step 4	<p>{deny permit} tcp</p> <p>Example:</p> <pre>{deny permit} tcp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length any hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port protocol}] [psh] [range{port protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]</pre>	<p>(Optional) Define a TCP access list and the access conditions. Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3, with these additional optional parameters:</p> <ul style="list-style-type: none"> • ack—Acknowledgment bit set. • established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set. • fin—Finished bit set; no more data from sender. • neq {port protocol}—Matches only packets that are not on a given port number. • psh—Push function bit set. • range {port protocol}—Matches only packets in the port number range. • rst—Reset bit set. • syn—Synchronize bit set. • urg—Urgent pointer bit set.
Step 5	<p>{deny permit} udp</p> <p>Example:</p> <pre>{deny permit} udp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length any hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input]</pre>	<p>(Optional) Define a UDP access list and the access conditions. Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.</p>

	Command or Action	Purpose
	<pre>[neg {port protocol}] [range {port protocol}] [routing][sequence value][time-range name]</pre>	
Step 6	<p>{deny permit} icmp</p> <p>Example:</p> <pre>{deny permit} icmp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length any hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]</pre>	<p>(Optional) Define an ICMP access list and the access conditions.</p> <p>Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:</p> <ul style="list-style-type: none"> • icmp-type—Enter to filter by ICMP message type, a number from 0 to 255. • icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255. • icmp-message—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.
Step 7	<p>end</p> <p>Example:</p> <pre>SwitchControllerDevice(config)# end</pre>	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 8	<p>show ipv6 access-list</p> <p>Example:</p> <pre>show ipv6 access-list</pre>	Verify the access list configuration.
Step 9	<p>copy running-config startup-config</p> <p>Example:</p> <pre>copy running-config startup-config</pre>	(Optional) Save your entries in the configuration file.

Applying an IPv6 ACL to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: SwitchControllerDevice# configure terminal	Enters global configuration mode.
Step 2	interface interface_id Example: SwitchControllerDevice# interface interface-id	Identify a Layer 2 interface (for port ACLs) or Layer 3 interface (for router ACLs) on which to apply an access list, and enter interface configuration mode.
Step 3	no switchport Example: SwitchControllerDevice# no switchport	If applying a router ACL, change the interface from Layer 2 mode (the default) to Layer 3 mode.
Step 4	ipv6 address ipv6_address Example: SwitchControllerDevice# ipv6 address ipv6-address	Configure an IPv6 address on a Layer 3 interface (for router ACLs). This command is not required on Layer 2 interfaces or if the interface has already been configured with an explicit IPv6 address.
Step 5	ipv6 traffic-filter access-list-name Example: SwitchControllerDevice# ipv6 traffic-filter access-list-name {in out}	Apply the access list to incoming or outgoing traffic on the interface. The out keyword is not supported for Layer 2 interfaces (port ACLs).
Step 6	end Example: SwitchControllerDevice(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.
Step 7	show running-config	Verify the access list configuration.
Step 8	copy running-config startup-config Example: copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Displaying IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands.

DETAILED STEPS

	Command or Action	Purpose
Step 1	show access-list Example: SwitchControllerDevice# show access-lists	Displays all access lists configured on the switchcontrollerdevice
Step 2	show ipv6 access-list <i>acl_name</i> Example: SwitchControllerDevice# show ipv6 access-list [<i>access-list-name</i>]	Displays all configured IPv6 access list or the access list specified by name.

Configuration Examples for IPv6 ACL

Example: Creating IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.



Note Logging is supported only on Layer 3 interfaces.

```
SwitchControllerDevice(config)# ipv6 access-list CISCO
SwitchControllerDevice(config-ipv6-acl)# deny tcp any any gt 5000
SwitchControllerDevice (config-ipv6-acl)# deny udp any any lt 5000 log
SwitchControllerDevice(config-ipv6-acl)# permit icmp any any
SwitchControllerDevice(config-ipv6-acl)# permit any any
```

Example: Applying IPv6 ACLs

This example shows how to apply the access list Cisco to outbound traffic on a Layer 3 interface.

```
SwitchControllerDevice(config)# interface TenGigabitEthernet 1/0/3
SwitchControllerDevice(config-if)# no switchport
SwitchControllerDevice(config-if)# ipv6 address 2001::/64 eui-64
SwitchControllerDevice(config-if)# ipv6 traffic-filter CISCO out
```

Example: Displaying IPv6 ACLs

This is an example of the output from the **show access-lists** privileged EXEC command. The output shows all access lists that are configured on the switch or switch stack.

```
SwitchControllerDevice #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

This is an example of the output from the **show ipv6 access-lists** privileged EXEC command. The output shows only IPv6 access lists configured on the switch or switch stack.

```
SwitchControllerDevice# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```



INDEX

128-bit [16](#)

A

ACLs [47](#)

address formats [16](#)

addresses [16](#)

IPv6 [16](#)

aggregatable global unicast addresses [17](#)
and IPv6 [17](#)

and switch stacks [20](#)

applications [18](#)

assigning address [21](#)

assigning IPv6 addresses to [21](#)

autoconfiguration [18](#)

C

Configuration Examples command [28](#)

Configuration Examples for Configuring MLD Snooping Queries
command [45](#)

Configuring a Multicast Router Port [45](#)

Example command [45](#)

Configuring a Static Multicast Group [45](#)

Example command [45](#)

Configuring IPv6 Addressing and Enabling IPv6 Routing [28](#)

Example command [28](#)

Configuring IPv6 ICMP Rate Limiting [28](#)

Example command [28](#)

Configuring MLD Snooping Queries [46](#)

Example command [46](#)

Configuring Static Routing for IPv6 [28](#)

Example command [28](#)

D

default configuration [21, 36](#)

IGMP snooping [36](#)

default configuration (*continued*)

IPv6 [21](#)

defined [16](#)

disabling [43](#)

Displaying IPv6 [29](#)

Example command [29](#)

DNS [17](#)

in IPv6 [17](#)

dual IPv4 and IPv6 templates [18](#)

dual protocol stacks [18](#)

IPv4 and IPv6 [18](#)

SDM templates supporting [18](#)

E

effects on [20](#)

IPv6 routing [20](#)

enabling [41](#)

enabling and disabling [37](#)

Enabling MLD Immediate Leave [46](#)

Example command [46](#)

EUI [17](#)

extended universal identifier [17](#)

See EUI [17](#)

F

forwarding [21](#)

H

HTTP(S) Over IPv6 [20](#)

I

ICMP [17](#)

IPv6 [17](#)

ICMPv6 [17](#)
 IGMP [41, 43, 44](#)
 leave processing, enabling [41](#)
 report suppression [43](#)
 disabling [43](#)
 snooping [44](#)
 IGMP snooping [36, 37, 44](#)
 default configuration [36](#)
 enabling and disabling [37](#)
 monitoring [44](#)
 Immediate Leave, IGMP [41](#)
 enabling [41](#)
 in IPv6 [17](#)
 Internet Protocol version 6 [16](#)
 See IPv6 [16](#)
 IP addresses [16](#)
 128-bit [16](#)
 IPv6 [16](#)
 IP unicast routing [17](#)
 IPv6 [17](#)
 IPv4 and IPv6 [18](#)
 IPv6 [16, 17, 18, 20, 21, 26, 31, 47](#)
 ACL [47](#)
 address formats [16](#)
 addresses [16](#)
 and switch stacks [20](#)
 applications [18](#)
 assigning address [21](#)
 autoconfiguration [18](#)
 default configuration [21](#)
 defined [16](#)
 forwarding [21](#)
 ICMP [17](#)
 monitoring [26](#)
 neighbor discovery [18](#)
 SDM templates [31](#)
 stack master functions [20](#)
 Stateless Autoconfiguration [18](#)
 supported features [17](#)
 IPv6 on [20](#)
 IPv6 routing [20](#)
 ISL [17](#)
 and IPv6 [17](#)

L

Layer 3 interfaces [21](#)
 assigning IPv6 addresses to [21](#)
 leave processing, enabling [41](#)
 link local unicast addresses [17](#)

M

MLD Messages [33](#)
 MLD Queries [33](#)
 MLD Reports [34](#)
 MLD Snooping [32](#)
 MLDv1 Done message [34](#)
 monitoring [26, 44](#)
 IGMP [44](#)
 snooping [44](#)
 IPv6 [26](#)
 Multicast Client Aging Robustness [34](#)
 multicast groups [39](#)
 static joins [39](#)
 Multicast Router Discovery [34](#)

N

neighbor discovery [18](#)
 neighbor discovery, IPv6 [18](#)

R

report suppression [43](#)
 disabling [43](#)
 report suppression, IGMP [43](#)
 disabling [43](#)

S

SDM templates [31](#)
 SDM templates supporting [18](#)
 See EUI [17](#)
 See IPv6 [16](#)
 SNMP and Syslog Over IPv6 [19](#)
 snooping [44](#)
 stack changes [20](#)
 effects on [20](#)
 IPv6 routing [20](#)
 stack master [20](#)
 IPv6 [20](#)
 stack master functions [20](#)
 stack member [20](#)
 IPv6 [20](#)
 stacks, switch [20](#)
 IPv6 on [20](#)
 Stateless Autoconfiguration [18](#)
 static joins [39](#)
 supported features [17](#)
 switch stacks [35](#)

T

Topology Change Notification Processing [35](#)

