IGMP Snooping and MVR Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 2960-X Switch)

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-32558-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

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.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`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.

Using the Command-Line Interface

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 switch 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 switch 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.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	`Switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Switch#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Switch(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 switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	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 switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Switch(config-if)#`		Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Switch(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	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:** `Switch# help`	Obtains a brief description of the help system in any command mode.

Step 2	*abbreviated-command-entry* **?**
	
	Example:
	`Switch# di?`
	`dir disable disconnect`
		Obtains a list of commands that begin with a particular character string.

Step 3	*abbreviated-command-entry* <Tab>
	
	Example:
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		Completes a partial command name.

Step 4	**?** **Example:** `Switch> ?`	Lists all commands available for a particular command mode.
Step 5	*command* **?** **Example:** `Switch> show ?`	Lists the associated keywords for a command.

Step 6	*command keyword* **?**
	
	Example:
	`Switch(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 switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# 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 switch.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your switch 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.
`% Incomplete command.`	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.
`% Invalid input detected at '^' marker.`	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 switch 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 switch 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** [**size** *number-of-lines*] **Example:** `Switch# terminal history size 200`	Changes the number of command lines that the switch 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.
Step 3	**show history** **Example:** `Switch# 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:** `Switch# 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: `Switch# terminal editing`	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	terminal no editing Example: `Switch# 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 switch 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	**access-list** **Example:** `Switch(config)# access-list 101 permit tcp`	Displays the global configuration command entry that extends beyond one line. 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

	Command or Action	Purpose
	10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# $ **101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25** Switch(config)# $**t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq** Switch(config)# $**15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45**	line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	**Ctrl-A** **Example:** Switch(config)# **access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$**	Checks the complete syntax. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	**Return** key	Execute the commands. 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. Use line wrapping with the command history feature to recall and modify previous complex command entries.

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	{**show**	**more**} *command*	{**begin**	**include**	**exclude**} *regular-expression* **Example:** Switch# **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	Searches and filters the output. 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.

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 switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch 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 switch. 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 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 switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

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

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

- Connect the switch 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 switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
    - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
    - The switch 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.

IGMP Snooping and MVR Commands

This chapter contains IGMP snooping and MVR commands.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Command Default

IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of the command.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

Syntax Description

vlan *vlan-id*	(Optional) Sets the count value on a specific VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
count	The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.

Command Default

A query is sent every 2 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response to the last-member queries are received before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.

Note Do not set the count to 1 because the loss of a single packet (the query packet from the switch to the host or the report packet from the host to the switch) may result in traffic forwarding being stopped even if there is still a receiver. Traffic continues to be forwarded after the next general query is sent by the switch, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last-member-query-interval (LMQI) value when the switch is processing more than one leave within an LMQI. In this case, the average leave latency is

determined by the (count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Examples

The following example sets the last member query count to 5:

```
Switch(config)# ip igmp snooping last-member-query-count 5
```

Related Commands

Command	Description
ip igmp snooping querier	Globally enables the IGMP querier function.
ip igmp snooping last-member-query-interval	Enables the IGMP configurable-leave timer.

ip igmp snooping last-member-query-interval

To enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis, use the **ip igmp snooping last-member-query-interval** command in global configuration mode. Use the **no** form of the command to return to the default setting.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval** *time*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval** *time*

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
time	Interval time out in seconds. The range is 100 to 32767 milliseconds.

Command Default

The default timeout setting is 1000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all the existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Configuring the leave timer on a VLAN overrides the global setting.

The IGMP configurable leave time is only supported on devices running IGMP Version 2.

The configuration is saved in NVRAM.

Examples

This example shows how to globally enable the IGMP leave timer for 2000 milliseconds:

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping last-member-query-count	Configures how many times IGMP snooping sends query messages in response to receiving an IGMP leave message.
ip igmp snooping querier	Globally enables the IGMP querier function.

ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]

no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
address *ip-address*	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
max-response-time *response-time*	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
query-interval *interval-count*	(Optional) Sets the interval between IGMP queriers. The range is 1 to 18000 seconds.
tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).
count *count*	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.
interval *interval*	Sets the TCN query interval time. The range is 1 to 255.
timer expiry *expiry-time*	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version *version*	(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.

Command Default

The IGMP snooping querier feature is globally disabled on the switch.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2) but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the max-response-time value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the max-response-time value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable the IGMP snooping querier feature:

```
Switch(config)# ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Switch(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Switch(config)# ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Switch(config)# ip igmp snooping querier timer expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Switch(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the switch stack or on a standalone switch. To disable IGMP report suppression and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

Examples

This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping configurations.

ip igmp snooping robustness-variable

To configure the IGMP robustness variable globally or on a per-VLAN basis, use the **ip igmp snooping robustness-variable** command in global configuration mode. Use the **no** form of the command to return to the default setting.

ip igmp snooping [**vlan** *vlan-id*] **robustness-variable** *number*

no ip igmp snooping [**vlan** *vlan-id*] **robustness-variable** *number*

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
number	Robustness variable number. The range is 1 to 3.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping configurations.

ip igmp snooping vlan immediate-leave

To enable IGMPv2 immediate leave processing, use the **immediate-leave** global configuration command on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Syntax Description

vlan-id	Enables IGMPv2 immediate leave processing in the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Command Default

By default, IGMPv2 immediate leave processing is off.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping configurations.
show mvr interface	Displays the configured MVR receiver and source ports with attributes and interface member groups.

ip igmp snooping vlan mrouter

To add a multicast router port or to configure the multicast learning method, use the **ip igmp snooping mrouter** global configuration command on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn** {**cgmp** | **pim-dvmrp**} }

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn** {**cgmp** | **pim-dvmrp**} }

Syntax Description

vlan-id	Enables IGMP snooping and adds the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094.
interface *interface-id*	Specifies the next-hop interface to the multicast router. The *interface-id* value has these options: • *fastethernet interface number*—A Fast Ethernet IEEE 802.3 interface. • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0 to 48.
learn	Specifies the multicast router learning method.
cgmp	Sets the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets.
pim-dvmrp	Sets the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets.

Command Default

By default, there are no multicast router ports.

The default learning method is pim-dvmrp to snoop IGMP queries and PIM-DVMRP packets.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The CGMP learn method is useful for reducing control traffic.

The configuration is saved in NVRAM.

Examples

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

This example shows how to specify the multicast router learning method as CGMP:

```
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** global configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to remove ports specified as members of a static multicast group.

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

vlan-id	Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
ip-address	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specifies the interface of the member port. The *interface-id* value has these options: • *fastethernet interface number*—A Fast Ethernet IEEE 802.3 interface. • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0 to 128.

Command Default

By default, there are no ports statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Examples

This example shows how to statically configure a host on an interface:

```
Switch(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

mvr (global configuration)

To enable the multicast VLAN registration (MVR) feature on the switch, use the **mvr** global configuration command without keywords on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

no mvr [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

Syntax Description

group *ip-address*	(Optional) Statically configures an MVR group IP multicast address on the switch. Use the **no** form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
count	(Optional) Multiple contiguous MVR group addresses. The range is 1 to 256; the default is 0.
mode	(Optional) Specifies the MVR mode of operation. The default is compatible mode.
compatible	(Optional) Sets MVR mode to provide compatibility with Catalyst 2900 XL and Catalyst 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
dynamic	(Optional) Sets MVR mode to allow dynamic MVR membership on source ports.
querytime *value*	(Optional) Sets the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from multicast group membership. The value is the response time in units of tenths of a second. The range is 1 to 100; the default is 5 tenths or one-half second. Use the **no** form of the command to return to the default setting.
vlan *vlan-id*	(Optional) Specifies the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094; the default is VLAN 1.

Command Default

MVR is disabled by default.

The default MVR **mode** is compatible mode.

No IP multicast addresses are configured on the switch by default.

The default **group** *ip-address count* is 0.

The default query response time is five-tenths or one-half second.

The default multicast VLAN for MVR is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

A maximum of 256 MVR multicast groups can be configured on a switch.

Use the command with keywords to set the MVR mode for a switch, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN.

Use the **mvr group** command to statically set up all the IP multicast addresses that will take part in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports that have registered to receive data on that IP multicast address.

MVR supports aliased IP multicast addresses on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).

The **mvr querytime** command applies only to receiver ports.

If the switch MVR is interoperating with Catalyst 2900 XL or Catalyst 3500 XL switches, set the multicast mode to compatible.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

MVR can coexist with IGMP snooping on a switch.

Multicast routing and MVR cannot coexist on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled and a warning message appears. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled with an error message.

Examples

This example shows how to enable MVR:

```
Switch(config)# mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

This example shows how to configure 228.1.23.4 as an IP multicast address:

```
Switch(config)# mvr group 228.1.23.4
```

This example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Switch(config)# mvr group 228.1.23.1 10
```

Use the **show mvr members** privileged EXEC command to display the IP multicast group addresses configured on the switch.

This example shows how to set the maximum query response time as one second (10 tenths):

```
Switch(config)# mvr querytime 10
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

You can verify your settings by entering the **show mvr** privileged EXEC command.

Related Commands

Command	Description
mvr (interface configuration)	Statically assigns and configures a port to an IP multicast VLAN and IP address.
show mvr	Displays the current MVR global or port parameter values.
show mvr interface	Displays the configured MVR receiver and source ports with attributes and interface member groups.
show mvr members	Displays all receiver and source ports that are currently members of an IP multicast group.

mvr (interface configuration)

To statically assign a port to an IP multicast VLAN and IP address, use the **mvr** interface configuration command on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

mvr [**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* **group** [*ip-address*]]

no mvr [**immediate** | **type** | **vlan** *vlan-id* **group** [*ip-address*]]

Syntax Description

immediate	(Optional) Enables the Immediate Leave feature of MVR on a port. Use the **no mvr immediate** command to disable the feature.
type	(Optional) Configures the port as an MVR receiver port or a source port. The default port type is neither an MVR source nor a receiver port. The **no mvr type** command resets the port as neither a source or a receiver port.
receiver	Configures the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.
source	Configures the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN.
vlan *vlan-id* **group**	(Optional) Adds the port as a static member of the multicast group with the specified VLAN ID. The **no mvr vlan** *vlan-id* **group** command removes a port on a VLAN from membership in an IP multicast address group.
ip-address	(Optional) Statically configures the specified MVR IP multicast group address for the specified multicast VLAN ID. This is the IP address of the multicast group that the port is joining.

Command Default

A port is configured as neither a receiver nor a source.

The Immediate Leave feature is disabled on all ports.

No receiver port is a member of any configured multicast group.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Configure a port as a source port if that port should be able to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Receiver ports cannot be trunk ports. Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.

A port that is not taking part in MVR should not be configured as an MVR receiver port or a source port. A non-MVR port is a normal switch port, able to send and receive multicast data with normal switch behavior.

When Immediate Leave is enabled, a receiver port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a group on a receiver port, it sends out an IGMP MAC-based query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP MAC-based query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency.

The Immediate Leave feature should be enabled only on receiver ports to which a single receiver device is connected.

The **mvr vlan group** command statically configures ports to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of group remains a member of the group until statically removed. In compatible mode, this command applies only to receiver ports; in dynamic mode, it can also apply to source ports. Receiver ports can also dynamically join multicast groups by using IGMP join messages.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

An MVR port cannot be a private-VLAN port.

Examples

This example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr type receiver
```

Use the **show mvr interface** privileged EXEC command to display configured receiver ports and source ports.

This example shows how to enable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mvr immediate
```

This example shows how to add a port on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

You can verify your settings by entering the **show mvr members** privileged EXEC command.

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registrations on the switch.
show mvr	Displays the current MVR global or port parameter values.
show mvr interface	Displays the configured MVR receiver and source ports with attributes and interface member groups.
show mvr members	Displays all receiver and source ports that are currently members of an IP multicast group.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN, use the **show ip igmp snooping** command in user or privileged EXEC command mode.

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description

groups	(Optional) Displays the IGMP snooping multicast table.
mrouter	(Optional) Displays the IGMP snooping multicast router ports.
querier	(Optional) Displays the configuration and operation information for the IGMP querier.
vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays operational state information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Switch# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
```

```
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
```

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch:

```
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Vlan 2:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
<output truncated>
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.
show ip igmp snooping mrouter	Displays the IGMP snooping multicast router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier.

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information, use the **show ip igmp snooping groups** privileged EXEC command.

show ip igmp snooping groups [**vlan** *vlan-id*] [[**dynamic** | **user**] [**count**] | *ip_address*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.
dynamic	(Optional) Displays IGMP snooping learned group information.
user	(Optional) Displays user-configured group information.
count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
ip_address	(Optional) Characteristics of the multicast group with the specified group IP address.

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch:

```
Switch# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi1/0/11
1         224.1.4.5       igmp                    Gi1/0/11
2         224.0.1.40      igmp        v2          Gi1/0/15
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3       igmp        v2          Gi2/0/1, Gi2/0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch:

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi1/0/15
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping	Displays IGMP snooping configurations.

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** privileged EXEC command.

show ip igmp snooping mrouter [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch:

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
show ip igmp snooping	Displays IGMP snooping configurations.
show ip igmp snooping groups	Displays the IGMP snooping multicast table.

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier configured on a switch, use the **show ip igmp snooping querier** user EXEC command.

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays detailed IGMP querier information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the switch, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier is learned in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the switch querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the switch querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version        Port
-----------------------------------------------------
1         172.20.50.11    v3                  Gi1/0/1
2         172.20.40.20    v2                  Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version    Port
-----------------------------------------------------------------
1         1.1.1.1         v2              Fa8/0/1
Global IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP switch querier status
-----------------------------------------------------------
elected querier is 1.1.1.1          on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping querier	Globally enables the IGMP querier function.
show ip igmp snooping	Displays IGMP snooping configurations.

show mvr

To display the current Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible), use the **show mvr** privileged EXEC command without keywords.

show mvr

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Examples

This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registrations on the switch.
mvr (interface configuration)	Statically assigns and configures a port to an IP multicast VLAN and IP address.
show mvr interface	Displays the configured MVR receiver and source ports with attributes and interface member groups.
show mvr members	Displays all receiver and source ports that are currently members of an IP multicast group.

show mvr interface

To display the Multicast VLAN Registration (MVR) receiver and source ports, use the **show mvr interface** privileged EXEC command without keywords. To display MVR parameters for a specific receiver port, use the command with keywords.

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]]

Syntax Description

interface-id	(Optional) Displays MVR type, status, and Immediate Leave setting for the interface. Valid interfaces include physical ports (including type, stack member (stacking-capable switches only) module, and port number).
members	(Optional) Displays all MVR groups to which the specified interface belongs.
vlan *vlan-id*	(Optional) Displays all MVR group members on this VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the interface appear. If you enter a VLAN ID, all MVR group members in the VLAN appear.

Examples

This is an example of output from the **show mvr interface** command:

```
Switch# show mvr interface
Port        Type            Status          Immediate Leave
----        ----            -------         ---------------
Gi1/0/1     SOURCE          ACTIVE/UP       DISABLED
Gi1/0/2     RECEIVER        ACTIVE/DOWN     DISABLED
```

In the preceding display, Status is defined as follows:

- Active means the port is part of a VLAN.
- Up/Down means that the port is forwarding/nonforwarding.

- Inactive means that the port is not yet part of any VLAN.

This is an example of output from the **show mvr interface** command for a specified port:

```
Switch# show mvr interface gigabitethernet1/0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface** *interface-id* **members** command:

```
Switch# show mvr interface gigabitethernet1/0/2 members
239.255.0.0     DYNAMIC ACTIVE
239.255.0.1     DYNAMIC ACTIVE
239.255.0.2     DYNAMIC ACTIVE
239.255.0.3     DYNAMIC ACTIVE
239.255.0.4     DYNAMIC ACTIVE
239.255.0.5     DYNAMIC ACTIVE
239.255.0.6     DYNAMIC ACTIVE
239.255.0.7     DYNAMIC ACTIVE
239.255.0.8     DYNAMIC ACTIVE
239.255.0.9     DYNAMIC ACTIVE
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registrations on the switch.
mvr (interface configuration)	Statically assigns and configures a port to an IP multicast VLAN and IP address.
show mvr	Displays the current MVR global or port parameter values.
show mvr members	Displays all receiver and source ports that are currently members of an IP multicast group.

show mvr members

To display all receiver and source ports that are currently members of an IP multicast group, use the **show mvr members** privileged EXEC command.

show mvr members [*ip-address*] [**vlan** *vlan-id*]

Syntax Description

ip-address	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.
vlan *vlan-id*	(Optional) Displays all MVR group members on this VLAN. The range is 1 to 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS 15.0(2)EX	This command was introduced.

Usage Guidelines

The **show mvr members** command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.

Examples

This is an example of output from the **show mvr members** command:

```
Switch# show mvr members
MVR Group IP    Status          Members
------------    ------          -------
239.255.0.1     ACTIVE          Gi1/0/1(d), Gi1/0/5(s)
239.255.0.2     INACTIVE        None
239.255.0.3     INACTIVE        None
239.255.0.4     INACTIVE        None
239.255.0.5     INACTIVE        None
239.255.0.6     INACTIVE        None
239.255.0.7     INACTIVE        None
239.255.0.8     INACTIVE        None
239.255.0.9     INACTIVE        None
239.255.0.10    INACTIVE        None
<output truncated>
```

This is an example of output from the **show mvr members** *ip-address* command. It displays the members of the IP multicast group with that address:

```
Switch# show mvr members 239.255.0.2
239.255.003.--22    ACTIVE        Gi1//1(d), Gi1/0/2(d), Gi1/0/3(d), Gi1/0/4(d), Gi1/0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registrations on the switch.
mvr (interface configuration)	Statically assigns and configures a port to an IP multicast VLAN and IP address.
show mvr	Displays the current MVR global or port parameter values.
show mvr interface	Displays the configured MVR receiver and source ports with attributes and interface member groups.

INDEX

I

M

S