



## **Network Management Command Reference, Cisco IOS Release 15.2(2)E (Catalyst 2960-XR 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-32588-01

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 NON-INFRINGEMENT 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

### Preface v

Document Conventions v

Related Documentation vii

Obtaining Documentation and Submitting a Service Request vii

---

### 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 4

No and Default Forms of Commands 5

CLI Error Messages 5

Configuration Logging 5

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

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

### Network Management Commands 15

debug platform ip dhcp 17

debug platform snmp	19
monitor session	20
monitor session destination	22
monitor session filter	26
monitor session source	28
show monitor session	31
show platform snmp counters	33
snmp-server enable traps	34
snmp-server enable traps bridge	37
snmp-server enable traps call-home	38
snmp-server enable traps cef	39
snmp-server enable traps cpu	41
snmp-server enable traps dot1x	42
snmp-server enable traps energywise	44
snmp-server enable traps envmon	46
snmp-server enable traps errdisable	48
snmp-server enable traps flash	49
snmp-server enable traps ike	50
snmp-server enable traps ipsec	52
snmp-server enable traps license	54
snmp-server enable traps mac-notification	55
snmp-server enable traps ospf	56
snmp-server enable traps pim	58
snmp-server enable traps port-security	59
snmp-server enable traps power-ethernet	60
snmp-server enable traps snmp	61
snmp-server enable traps stackwise	63
snmp-server enable traps storm-control	66
snmp-server enable traps stpx	67
snmp-server enable traps transceiver	68
snmp-server enable traps vstack	69
snmp-server engineID	71
snmp-server host	72



## Preface

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

## 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 <b>^D</b> or <b>Ctrl-D</b> 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.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<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> .
<b>Bold Courier font</b>	<b>Bold Courier font</b> 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 switch release notes.

---

- Catalyst 2960-XR Switch documentation, located at:  
[http://www.cisco.com/go/cat2960xr\\_docs](http://www.cisco.com/go/cat2960xr_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](http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html)
- Error Message Decoder, located at:  
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

## 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, 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 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 <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Switch#	Enter <b>disable</b> 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 <b>configure</b> command.	Switch(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the <b>vlan <i>vlan-id</i></b> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command.  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	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 <b>interface</b> 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 <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	
Line configuration	While in global configuration mode, specify a line with the <b>line vty</b> or <b>line console</b> command.	Switch(config-line)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	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	<b>help</b>  <b>Example:</b> Switch# <b>help</b>	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i>  <b>Example:</b> Switch# <b>di?</b> dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry &lt;Tab&gt;</i>  <b>Example:</b> Switch# <b>sh conf&lt;tab&gt;</b> Switch# <b>show configuration</b>	Completes a partial command name.
Step 4	<b>?</b>  <b>Example:</b> Switch> <b>?</b>	Lists all commands available for a particular command mode.
Step 5	<i>command ?</i>  <b>Example:</b> Switch> <b>show ?</b>	Lists the associated keywords for a command.
Step 6	<i>command keyword ?</i>  <b>Example:</b> Switch(config)# <b>cdp holdtime ?</b> <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
<b>Step 1</b>	<b>terminal history [size number-of-lines]</b>  <b>Example:</b> Switch# <code>terminal history size 200</code>	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
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> Switch# <b>show history</b>	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 <b>terminal history</b> global configuration command and the <b>history</b> 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
<b>Step 1</b>	<b>terminal no history</b>  <b>Example:</b> Switch# <b>terminal no history</b>	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 reenble it.

**SUMMARY STEPS**

1. `terminal editing`
2. `terminal no editing`

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>terminal editing</code>  <b>Example:</b> Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
<b>Step 2</b>	<code>terminal no editing</code>  <b>Example:</b> Switch# <code>terminal no editing</code>	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
<b>Ctrl-B</b> or use the <b>left arrow</b> key	Moves the cursor back one character.
<b>Ctrl-F</b> or use the <b>right arrow</b> key	Moves the cursor forward one character.
<b>Ctrl-A</b>	Moves the cursor to the beginning of the command line.
<b>Ctrl-E</b>	Moves the cursor to the end of the command line.
<b>Esc B</b>	Moves the cursor back one word.
<b>Esc F</b>	Moves the cursor forward one word.
<b>Ctrl-T</b>	Transposes the character to the left of the cursor with the character located at the cursor.
<b>Delete</b> or <b>Backspace</b> key	Erases the character to the left of the cursor.
<b>Ctrl-D</b>	Deletes the character at the cursor.
<b>Ctrl-K</b>	Deletes all characters from the cursor to the end of the command line.
<b>Ctrl-U</b> or <b>Ctrl-X</b>	Deletes all characters from the cursor to the beginning of the command line.
<b>Ctrl-W</b>	Deletes the word to the left of the cursor.
<b>Esc D</b>	Deletes from the cursor to the end of the word.
<b>Esc C</b>	Capitalizes at the cursor.
<b>Esc L</b>	Changes the word at the cursor to lowercase.
<b>Esc U</b>	Capitalizes letters from the cursor to the end of the word.

<b>Ctrl-V</b> or <b>Esc Q</b>	Designates a particular keystroke as an executable command, perhaps as a shortcut.
<b>Return</b> key	Scrolls down a line or screen on displays that are longer than the terminal screen can display.  <b>Note</b> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <b>show</b> command output. You can use the <b>Return</b> and <b>Space</b> bar keystrokes whenever you see the More prompt.
<b>Space</b> bar	Scrolls down one screen.
<b>Ctrl-L</b> or <b>Ctrl-R</b>	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
<b>Step 1</b>	<b>access-list</b>  <b>Example:</b> Switch(config)# <b>access-list 101 permit tcp</b>	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
	<pre>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</pre>	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	<p><b>Ctrl-A</b></p> <p><b>Example:</b></p> <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</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	<b>Return key</b>	<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 <b>terminal width</b> 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	<pre>{show   more} command   {begin   include   exclude} regular-expression</pre> <p><b>Example:</b></p> <pre>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</pre>	<p>Searches and filters the output.</p> <p>Expressions are case sensitive. For example, if you enter <b>  exclude output</b>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>OUTPUT</b> 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 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.







## Network Management Commands

---

- [debug platform ip dhcp](#), page 17
- [debug platform snmp](#), page 19
- [monitor session](#), page 20
- [monitor session destination](#), page 22
- [monitor session filter](#), page 26
- [monitor session source](#), page 28
- [show monitor session](#), page 31
- [show platform snmp counters](#), page 33
- [snmp-server enable traps](#), page 34
- [snmp-server enable traps bridge](#), page 37
- [snmp-server enable traps call-home](#), page 38
- [snmp-server enable traps cef](#), page 39
- [snmp-server enable traps cpu](#), page 41
- [snmp-server enable traps dot1x](#), page 42
- [snmp-server enable traps energywise](#), page 44
- [snmp-server enable traps envmon](#), page 46
- [snmp-server enable traps errdisable](#), page 48
- [snmp-server enable traps flash](#), page 49
- [snmp-server enable traps ike](#), page 50
- [snmp-server enable traps ipsec](#), page 52
- [snmp-server enable traps license](#), page 54
- [snmp-server enable traps mac-notification](#), page 55
- [snmp-server enable traps ospf](#), page 56
- [snmp-server enable traps pim](#), page 58

- [snmp-server enable traps port-security, page 59](#)
- [snmp-server enable traps power-ethernet, page 60](#)
- [snmp-server enable traps snmp, page 61](#)
- [snmp-server enable traps stackwise, page 63](#)
- [snmp-server enable traps storm-control, page 66](#)
- [snmp-server enable traps stpx, page 67](#)
- [snmp-server enable traps transceiver, page 68](#)
- [snmp-server enable traps vstack, page 69](#)
- [snmp-server engineID, page 71](#)
- [snmp-server host, page 72](#)

# debug platform ip dhcp

To debug DHCP events, use the **debug platform ip dhcp** command in user or privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug platform ip dhcp** {all | error | event | packet | rpc}

**no debug platform ip dhcp** {all | error | event | packet | rpc}

## Syntax Description

<b>all</b>	Displays all DHCP debug messages.
<b>error</b>	Displays DHCP error debug messages.
<b>event</b>	Displays DHCP event debug messages.
<b>packet</b>	Displays DHCP packet-related debug messages.
<b>rpc</b>	Displays DHCP remote procedure call (RPC) request debug messages.

## Command Default

Debugging is disabled.

## Command Modes

User EXEC

Privileged EXEC

## Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

## Usage Guidelines

The **undebg platform ip dhcp** command is the same as the **no debug platform ip dhcp** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the stack master by using the **session switch-number** EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** EXEC command on the active switch to enable debugging on a member switch without first starting a session.

## Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding information.

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

# debug platform snmp

To enable debugging of the platform-dependent Simple Network Management Protocol (SNMP) software, use the **debug platform snmp** command in user or privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug platform snmp**

**no debug platform snmp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Debugging is disabled.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines** The **undebug platform snmp** command is the same as the **no debug platform snmp** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session switch-number EXEC** command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE EXEC** command on the active switch to enable debugging on a member switch without first starting a session.

Related Commands	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.

## monitor session

To create a new Ethernet Switched Port Analyzer (SPAN) or a Remote Switched Port Analyzer (RSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear SPAN or RSPAN sessions, use the **no** form of this command.

**monitor session** *session-number* {**destination** | **filter** | **source**}

**no monitor session** {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

### Syntax Description

<i>session-number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
<b>all</b>	Clears all monitor sessions.
<b>local</b>	Clears all local monitor sessions.
<b>range</b> <i>session-range</i>	Clears monitor sessions in the specified range.
<b>remote</b>	Clears all remote monitor sessions.

### Command Default

No monitor sessions are configured.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

A private-VLAN port cannot be configured as a SPAN destination port.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

## Examples

This example shows how to create a local SPAN session 1 to monitor traffic on Po13 (an Etherchannel port) and limit SPAN traffic in the session only to VLAN 1281. Egress traffic replicates the source; ingress forwarding is not enabled.

```
Switch(config)# monitor session 1 source interface Po13
Switch(config)# monitor session 1 filter vlan 1281
Switch(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
replicate
Switch(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
replicate
```

The following is the output of a **show monitor session all** command after completing these setup instructions:

```
Switch# show monitor session all

Session 1
-----
Type                : Local Session
Source Ports        :
  Both              : Po13
Destination Ports   : Gi2/0/36,Gi3/0/36
  Encapsulation     : Replicate
  Ingress           : Disabled
Filter VLANs        : 1281
...
```

## monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

**monitor session** *session-number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**replicate** | **dot1q**} ] {**ingress** [**dot1q** | **untagged**] } | **remote**} **vlan** *vlan-id*

**no monitor session** *session-number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**replicate** | **dot1q**} ] {**ingress** [**dot1q** | **untagged**] } | **remote**} **vlan** *vlan-id*

### Syntax Description

<i>session-number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
<b>interface</b> <i>interface-id</i>	Specifies the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For <b>source interface</b> , <b>port channel</b> is also a valid interface type, and the valid range is 1 to 48.
,	(Optional) Specifies a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
<b>encapsulation replicate</b>	(Optional) Specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).  These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The <b>encapsulation</b> options are ignored with the <b>no</b> form of the command.
<b>encapsulation dot1q</b>	(Optional) Specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation.  These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The <b>encapsulation</b> options are ignored with the <b>no</b> form of the command.

<b>ingress</b>	(Optional) Enables ingress traffic forwarding.
<b>dot1q vlan</b> <i>vlan-id</i>	Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
<b>isl</b>	Specifies ingress forwarding using ISL encapsulation.
<b>untagged vlan</b> <i>vlan-id</i>	Accepts incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.
<b>vlan</b> <i>vlan-id</i>	When used with only the <b>ingress</b> keyword, sets the default VLAN for ingress traffic.
<b>remote vlan</b> <i>vlan-id</i>	Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.  The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
<b>all, local, range, and remote</b>	Specifies <b>all</b> , <b>local</b> , <b>range</b> <i>session-range</i> , or <b>remote</b> with the <b>no monitor session</b> command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.

**Command Default**

No monitor sessions are configured.

If **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

**Command Modes**

Global configuration

**Command History**

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines**

You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

A SPAN or RSPAN destination must be a physical port.

You can have a maximum of 64 destination ports on a switch or a switch stack.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [, | -] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (-).

EtherChannel ports cannot be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A private-VLAN port cannot be configured as a SPAN destination port.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x authentication is disabled until the port is removed as a SPAN destination. If IEEE 802.1x authentication is not available on the port, the switch returns an error message. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to act in these ways:

- When you enter **monitor session** *session\_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.
- When you enter **monitor session** *session\_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**.
- When you enter **monitor session** *session\_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
- When you enter **monitor session** *session\_number* **destination interface** *interface-id* **encapsulation replicate ingress**, egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

## Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Switch(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor a source interface and to configure the destination RSPAN VLAN 900:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
vlan 5
```

## monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

**monitor session** *session-number* **filter** {**vlan** *vlan-id* [, | -] | {**ip** | **ipv6** | **mac**} **access-group** *access-list*}

**no monitor session** *session-number* **filter** {**vlan** *vlan-id* [, | -] | {**ip** | **ipv6** | **mac**} **access-group** *access-list*}

### Syntax Description

<i>session-number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
<b>vlan</b> <i>vlan-id</i>	Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The <i>vlan-id</i> range is 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separates a range of VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.

### Command Default

No monitor sessions are configured.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [, | -] options.

If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (-).

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session *session\_number* filter vlan *vlan-id*** command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

## Examples

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2 and to filter IPv4 traffic using access list number 122 in an FSPAN session:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

## monitor session source

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source session, or to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session source** global configuration command. To remove the SPAN or RSPAN session or to remove source interfaces from the SPAN or RSPAN session use the **no** form of this command.

**monitor session** *session\_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}

**no monitor session** *session\_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}

### Syntax Description

<i>session_number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, the range is 1 to 66.
<b>interface</b> <i>interface-id</i>	Specifies the source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For <b>source interface</b> , <b>port channel</b> is also a valid interface type, and the valid range is 1 to 48.
,	(Optional) Specifies a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
<b>both, rx, tx</b>	(Optional) Specifies the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
<b>remote vlan</b> <i>vlan-id</i>	Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.  The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
<b>vlan</b> <i>vlan-id</i>	When used with only the <b>ingress</b> keyword, sets default VLAN for ingress traffic.

### Command Default

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines**

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

You can set a combined maximum of four local SPAN sessions and RSPAN source sessions. You can have a total of 68 SPAN and RSPAN sessions on a switch or switch stack. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.

A source can be a physical port, a port channel, or a VLAN.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [,|-] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (-).

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

**Examples**

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
```

```
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

## show monitor session

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor session** command in EXEC mode.

**show monitor session** {*session\_number* | **all** | **erspan-destination** | **erspan-source** | **local** | **range list** | **remote**} [**detail**]

### Syntax Description

<i>session_number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.
<b>all</b>	Displays all SPAN sessions.
<b>erspan-destination</b>	Displays only destination ERSPAN sessions.
<b>erspan-source</b>	Displays only source ERSPAN sessions.
<b>local</b>	Displays only local SPAN sessions.
<b>range list</b>	Displays a range of SPAN sessions, where <i>list</i> is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.  <b>Note</b> This keyword is available only in privileged EXEC mode.
<b>remote</b>	Displays only remote SPAN sessions.
<b>detail</b>	(Optional) Displays detailed information about the specified sessions.

### Command Modes

User EXEC  
Privileged EXEC

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines**

Maximum number of SPAN source sessions: 4 (applies to source and local sessions) However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions.

**Examples**

This is an example of output for the **show monitor session** privileged EXEC command for local SPAN source session 1:

```
Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

This is an example of output for the **show monitor session all** privileged EXEC command when ingress traffic forwarding is enabled:

```
Switch# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

# show platform snmp counters

To display platform-dependent Simple Network Management Protocol (SNMP) counter information, use the **show platform snmp counters** privileged EXEC command.

```
show platform snmp counters
```

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines** Use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

## snmp-server enable traps

To enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps** [auth-framework [sec-violation] | bridge | call-home | cef | cluster | config | config-copy | config-ctid | copy-config | cpu | dot1x | eigrp | energywise | entity | envmon | errdisable | event-manager | flash | fru-ctrl | hsrp | ike | ipmulticast | ipsec | license | mac-notification | ospf | pim | port-security | power-ethernet | rep | snmp | stackwise | storm-control | stpx | syslog | transceiver | tty | vlan-membership | vlancreate | vlandelete | vstack | vtp ]

**no snmp-server enable traps** [auth-framework | bridge | call-home | cef | cluster | config | config-copy | config-ctid | copy-config | cpu | dot1x | eigrp | energywise | entity | envmon | errdisable | event-manager | flash | fru-ctrl | hsrp | ike | ipmulticast | ipsec | license | mac-notification | ospf | pim | port-security | power-ethernet | rep | snmp | stackwise | storm-control | stpx | syslog | transceiver | tty | vlan-membership | vlancreate | vlandelete | vstack | vtp ]

### Syntax Description

<b>auth-framework</b>	(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
<b>sec-violation</b>	(Optional) Enables SNMP camSecurityViolationNotif notifications.
<b>bridge</b>	(Optional) Enables SNMP STP Bridge MIB traps.*
<b>call-home</b>	(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.*
<b>cef</b>	(Optional) Enables cluster traps.*
<b>cluster</b>	(Optional) Enables SNMP cluster traps.
<b>config</b>	(Optional) Enables SNMP configuration traps.
<b>config-copy</b>	(Optional) Enables SNMP configuration copy traps.
<b>config-ctid</b>	(Optional) Enables SNMP configuration CTID traps.
<b>copy-config</b>	(Optional) Enables SNMP copy-configuration traps.
<b>cpu</b>	(Optional) Enables CPU notification traps.*
<b>dot1x</b>	(Optional) Enables SNMP dot1x traps.*
<b>eigrp</b>	(Optional) Enables SNMP EIGRP traps.
<b>energywise</b>	(Optional) Enables SNMP energywise traps.*
<b>entity</b>	(Optional) Enables SNMP entity traps.

<b>envmon</b>	(Optional) Enables SNMP environmental monitor traps.*
<b>errdisable</b>	(Optional) Enables SNMP errdisable notification traps.*
<b>event-manager</b>	(Optional) Enables SNMP Embedded Event Manager traps.
<b>flash</b>	(Optional) Enables SNMP FLASH notification traps.*
<b>fru-ctrl</b>	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a switch stack, this trap refers to the insertion or removal of a switch in the stack.
<b>hsrp</b>	(Optional) Enables SNMP HSRP traps.
<b>ike</b>	(Optional) Enables SNMP IKE traps.*
<b>ipmulticast</b>	(Optional) Enables IP multicast routing traps.
<b>ipsec</b>	(Optional) Enables SNMP IPsec traps.*
<b>license</b>	(Optional) Enables license traps.*
<b>mac-notification</b>	(Optional) Enables SNMP MAC Notification traps.*
<b>ospf</b>	(Optional) Enables OSPF traps.*
<b>pim</b>	(Optional) Enables SNMP PIM traps.*
<b>port-security</b>	(Optional) Enables SNMP port security traps.*
<b>power-ethernet</b>	(Optional) Enables SNMP power Ethernet traps.*
<b>rep</b>	(Optional) Enables SNMP Resilient Ethernet Protocol traps.
<b>snmp</b>	(Optional) Enables SNMP traps.*
<b>stackwise</b>	(Optional) Enables SNMP stackwise traps.*
<b>storm-control</b>	(Optional) Enables SNMP storm-control trap parameters.*
<b>stp</b>	(Optional) Enables SNMP STP MIB traps.*
<b>syslog</b>	(Optional) Enables SNMP syslog traps.
<b>transceiver</b>	(Optional) Enables SNMP transceiver traps.*
<b>tty</b>	(Optional) Sends TCP connection traps. This is enabled by default.
<b>vlan-membership</b>	(Optional) Enables SNMP VLAN membership traps.
<b>vlancreate</b>	(Optional) Enables SNMP VLAN-created traps.

<b>vdelete</b>	(Optional) Enables SNMP VLAN-deleted traps.
<b>vstack</b>	(Optional) Enables SNMP Smart Install traps.*
<b>vtp</b>	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

**Command Default** The sending of SNMP traps is disabled.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines** The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.



**Note** Though visible in the command-line help strings, the **fru-ctrl**, **insertion**, and **removal** keywords are not supported on the switch. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host *host-addr* informs** global configuration command.



**Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

**Examples** This example shows how to enable more than one type of SNMP trap:

```
Switch(config)# snmp-server enable traps cluster
Switch(config)# snmp-server enable traps config
Switch(config)# snmp-server enable traps vtp
```

# snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps bridge** [**newroot**] [**topologychange**]

**no snmp-server enable traps bridge** [**newroot**] [**topologychange**]

## Syntax Description

<b>newroot</b>	(Optional) Enables SNMP STP bridge MIB new root traps.
<b>topologychange</b>	(Optional) Enables SNMP STP bridge MIB topology change traps.

## Command Default

The sending of bridge SNMP traps is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

## Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

## Examples

This example shows how to send bridge new root traps to the NMS:

```
Switch(config)# snmp-server enable traps bridge newroot
```

## Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps call-home

To enable SNMP CISCO-CALLHOME-MIB traps, use the **snmp-server enable traps call-home** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps call-home** [**message-send-fail** | **server-fail**]

**no snmp-server enable traps call-home** [**message-send-fail** | **server-fail**]

### Syntax Description

<b>message-send-fail</b>	(Optional) Enables SNMP message-send-fail traps.
<b>server-fail</b>	(Optional) Enables SNMP server-fail traps.

### Command Default

The sending of SNMP CISCO-CALLHOME-MIB traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate SNMP message-send-fail traps:

```
Switch(config)# snmp-server enable traps call-home message-send-fail
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps cef

To enable SNMP Cisco Express Forwarding (CEF) traps, use the **snmp-server enable traps cef** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps cef [inconsistency | peer-fib-state-change | peer-state-change | resource-failure]
no snmp-server enable traps cef [inconsistency | peer-fib-state-change | peer-state-change | resource-failure]
```

### Syntax Description

<b>inconsistency</b>	(Optional) Enables SNMP CEF Inconsistency traps.
<b>peer-fib-state-change</b>	(Optional) Enables SNMP CEF Peer FIB State change traps.
<b>peer-state-change</b>	(Optional) Enables SNMP CEF Peer state change traps.
<b>resource-failure</b>	(Optional) Enables SNMP CEF Resource Failure traps.

### Command Default

The sending of SNMP CEF traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate SNMP CEF inconsistency traps:

```
Switch(config)# snmp-server enable traps cef inconsistency
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps cpu** [threshold]

**no snmp-server enable traps cpu** [threshold]

<b>Syntax Description</b>	<b>threshold</b> (Optional) Enables CPU threshold notification.
---------------------------	---

<b>Command Default</b>	The sending of CPU notifications is disabled.
------------------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS 15.0(2)EX1	This command was introduced.

<b>Usage Guidelines</b>	Specify the host (NMS) that receives the traps by using the <b>snmp-server host</b> global configuration command. If no trap types are specified, all trap types are sent.
-------------------------	--



### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

<b>Examples</b>	This example shows how to generate CPU threshold notifications:
-----------------	---

```
Switch(config)# snmp-server enable traps cpu threshold
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps dot1x

To enable IEEE 802.1x traps, use the **snmp-server enable traps dot1x** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps dot1x** [**auth-fail-vlan**][**guest-vlan**][**no-auth-fail-vlan**][**no-guest-vlan**]

**no snmp-server enable traps dot1x** [**auth-fail-vlan**][**guest-vlan**][**no-auth-fail-vlan**][**no-guest-vlan**]

### Syntax Description

<b>auth-fail-vlan</b>	(Optional) Generates a trap when the port moves to the configured restricted VLAN.
<b>guest-vlan</b>	(Optional) Generates a trap when the port moves to the configured guest VLAN.
<b>no-auth-fail-vlan</b>	(Optional) Generates a trap when a port tries to enter the restricted VLAN, but cannot because the restricted VLAN is not configured.
<b>no-guest-vlan</b>	(Optional) Generates a trap when a port tries to enter the guest VLAN, but cannot because the guest VLAN is not configured.

### Command Default

The sending of IEEE 802.1x SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

When the **snmp-server enable traps dot1x** command is entered (without any other keywords specified), all the IEEE 802.1x traps are enabled.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

**Examples**

This example shows how to generate a trap when the port moves to the configured restricted VLAN:

```
Switch(config)# snmp-server enable traps dot1x auth-fail-vlan
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps energywise

To enable SNMP Energywise traps, use the **snmp-server enable traps energywise** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps energywise [event-occured][level-change][neighbor-added][neighbor-deleted]
no snmp-server enable traps energywise [event-occured][level-change][neighbor-added][neighbor-deleted]
```

### Syntax Description

<b>event-occured</b>	(Optional) Enables Energywise event occurred traps.
<b>level-change</b>	(Optional) Enables Energywise entity level change traps.
<b>neighbor-added</b>	(Optional) Enables Energywise entity neighbor added traps.
<b>neighbor-deleted</b>	(Optional) Enables Energywise entity neighbor deleted traps.

### Command Default

The sending of SNMP Energywise traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

When the **snmp-server enable traps energywise** command is entered (without any other keywords specified), all the SNMP Energywise traps are enabled.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate a trap when an Energywise event occurs:

```
Switch(config)# snmp-server enable traps energywise event-occured
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps envmon** [**fan**][**shutdown**][**status**] [**supply**][**temperature**]

**no snmp-server enable traps envmon** [**fan**][**shutdown**][**status**] [**supply**][**temperature**]

### Syntax Description

<b>fan</b>	(Optional) Enables fan traps.
<b>shutdown</b>	(Optional) Enables environmental monitor shutdown traps.
<b>status</b>	(Optional) Enables SNMP environmental status-change traps.
<b>supply</b>	(Optional) Enables environmental monitor power-supply traps.
<b>temperature</b>	(Optional) Enables environmental monitor temperature traps.

### Command Default

The sending of environmental SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate fan traps:

```
Switch(config)# snmp-server enable traps envmon fan
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps errdisable** [**notification-rate** *number-of-notifications*]

**no snmp-server enable traps errdisable** [**notification-rate** *number-of-notifications*]

### Syntax Description

<b>notification-rate</b> <i>number-of-notifications</i>	(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.
--	--

### Command Default

The sending of SNMP notifications of error-disabling is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to set the number SNMP notifications of error-disabling to 2:

```
Switch(config)# snmp-server enable traps errdisable notification-rate 2
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

# snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps flash** [insertion][removal]

**no snmp-server enable traps flash** [insertion][removal]

## Syntax Description

<b>insertion</b>	(Optional) Enables SNMP flash insertion notifications.
<b>removal</b>	(Optional) Enables SNMP flash removal notifications.

## Command Default

The sending of SNMP flash notifications is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

## Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

## Examples

This example shows how to generate SNMP flash insertion notifications:

```
Switch(config)# snmp-server enable traps flash insertion
```

## Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps ike

To enable IKE traps, use the **snmp-server enable traps ike** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps ike** {policy {add | delete} | tunnel {start | stop}}

**no snmp-server enable traps ike** {policy {add | delete} | tunnel {start | stop}}

### Syntax Description

<b>policy</b>	(Optional) Enables IKE policy traps.
<b>add</b>	(Optional) Enables IKE policy add traps.
<b>delete</b>	(Optional) Enables IKE policy delete traps.
<b>tunnel</b>	(Optional) Enables IKE tunnel traps.
<b>start</b>	(Optional) Enables IKE tunnel start traps.
<b>stop</b>	(Optional) Enables IKE tunnel stop traps.

### Command Default

The sending of IKE traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

**Examples**

This example shows how to generate IKE tunnel start traps:

```
Switch(config)# snmp-server enable traps ike tunnel start
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps ipsec

To enable IPsec traps, use the **snmp-server enable traps ipsec** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps ipsec** {cryptomap {add | attach | delete | detach} | too-many-sas | tunnel {start | stop}}

**no snmp-server enable traps ipsec** {cryptomap {add | attach | delete | detach} | too-many-sas | tunnel {start | stop}}

### Syntax Description

<b>cryptomap</b>	Enables IPsec Cryptomap traps.
<b>add</b>	Enables IPsec Cryptomap add traps.
<b>attach</b>	Enables IPsec Cryptomap attach traps.
<b>delete</b>	Enables IPsec Cryptomap delete traps.
<b>detach</b>	Enables IPsec Cryptomap detach traps.
<b>too-many-sas</b>	Enables IPsec too-many-sas traps.
<b>tunnel</b>	Enables IPsec tunnel traps.
<b>start</b>	Enables IPsec tunnel start traps.
<b>stop</b>	Enables IPsec tunnel stop traps.

### Command Default

The sending of IPsec traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

**Note**

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

**Examples**

This example shows how to generate IPsec tunnel start traps:

```
Switch(config)# snmp-server enable traps ipsec tunnel start
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps license

To enable license traps, use the **snmp-server enable traps license** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps license** [**deploy**][**error**][**usage**]

**no snmp-server enable traps license** [**deploy**][**error**][**usage**]

### Syntax Description

<b>deploy</b>	(Optional) Enables license deployment traps.
<b>error</b>	(Optional) Enables license error traps.
<b>usage</b>	(Optional) Enables license usage traps.

### Command Default

The sending of license traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate license deployment traps:

```
Switch(config)# snmp-server enable traps license deploy
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps mac-notification** [**change**][**move**][**threshold**]

**no snmp-server enable traps mac-notification** [**change**][**move**][**threshold**]

### Syntax Description

<b>change</b>	(Optional) Enables SNMP MAC change traps.
<b>move</b>	(Optional) Enables SNMP MAC move traps.
<b>threshold</b>	(Optional) Enables SNMP MAC threshold traps.

### Command Default

The sending of SNMP MAC notification traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate SNMP MAC notification change traps:

```
Switch(config)# snmp-server enable traps mac-notification change
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps ospf

To enable SNMP Open Shortest Path First (OSPF) traps, use the **snmp-server enable traps ospf** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time* *max-number-of-traps* | **retransmit** | **state-change**]

**no snmp-server enable traps ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time* *max-number-of-traps* | **retransmit** | **state-change**]

### Syntax Description

<b>cisco-specific</b>	(Optional) Enables Cisco-specific traps.
<b>errors</b>	(Optional) Enables error traps.
<b>lsa</b>	(Optional) Enables link-state advertisement (LSA) traps.
<b>rate-limit</b>	(Optional) Enables rate-limit traps.
<i>rate-limit-time</i>	(Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.
<i>max-number-of-traps</i>	(Optional) Specifies maximum number of rate-limit traps to be sent in window time.
<b>retransmit</b>	(Optional) Enables packet-retransmit traps.
<b>state-change</b>	(Optional) Enables state-change traps.

### Command Default

The sending of OSPF SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

**Note**

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

**Examples**

This example shows how to enable LSA traps:

```
Switch(config)# snmp-server enable traps ospf lsa
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps pim

To enable SNMP Protocol-Independent Multicast (PIM) traps, use the **snmp-server enable traps pim** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps pim** [**invalid-pim-message**][**neighbor-change**][**rp-mapping-change**]

**no snmp-server enable traps pim** [**invalid-pim-message**][**neighbor-change**][**rp-mapping-change**]

### Syntax Description

<b>invalid-pim-message</b>	(Optional) Enables invalid PIM message traps.
<b>neighbor-change</b>	(Optional) Enables PIM neighbor-change traps.
<b>rp-mapping-change</b>	(Optional) Enables rendezvous point (RP)-mapping change traps.

### Command Default

The sending of PIM SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to enable invalid PIM message traps:

```
Switch(config)# snmp-server enable traps pim invalid-pim-message
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps port-security

To enable SNMP port security traps, use the **snmp-server enable traps port-security** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps port-security** [*trap-rate value*]

**no snmp-server enable traps port-security** [*trap-rate value*]

### Syntax Description

<b>trap-rate</b> <i>value</i>	(Optional) Sets the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every occurrence).
-------------------------------	--

### Command Default

The sending of port security SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to enable port-security traps at a rate of 200 per second:

```
Switch(config)# snmp-server enable traps port-security trap-rate 200
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps power-ethernet

To enable SNMP power-over-Ethernet (PoE) traps, use the **snmp-server enable traps power-ethernet** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps power-ethernet** {group *number* | **police**}

**no snmp-server enable traps power-ethernet** {group *number* | **police**}

### Syntax Description

<b>group</b> <i>number</i>	Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.
<b>police</b>	Enables inline power policing traps.

### Command Default

The sending of power-over-Ethernet SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to enable power-over-Ethernet traps for group 1:

```
Switch(config)# snmp-server enable traps power-over-ethernet group 1
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps snmp** [**authentication** ][**coldstart** ][**linkdown** ] [**linkup** ][**warmstart**]

**no snmp-server enable traps snmp** [**authentication** ][**coldstart** ][**linkdown** ] [**linkup** ][**warmstart**]

### Syntax Description

<b>authentication</b>	(Optional) Enables authentication traps.
<b>coldstart</b>	(Optional) Enables cold start traps.
<b>linkdown</b>	(Optional) Enables linkdown traps.
<b>linkup</b>	(Optional) Enables linkup traps.
<b>warmstart</b>	(Optional) Enables warmstart traps.

### Command Default

The sending of SNMP traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to enable a warmstart SNMP trap:

```
Switch(config)# snmp-server enable traps snmp warmstart
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps stackwise

To enable SNMP StackWise traps, use the **snmp-server enable traps stackwise** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps stackwise [GLS][ILS][SRLS] [insufficient-power][invalid-input-current]
[invalid-output-current][member-removed][member-upgrade-notification] [new-master][new-member]
[port-change][power-budget-warning][power-invalid-topology]
[power-link-status-changed][power-oper-status-changed]
[power-priority-conflict][power-version-mismatch][ring-redundant]
[stack-mismatch][unbalanced-power-supplies][under-budget][under-voltage]
```

```
no snmp-server enable traps stackwise [GLS][ILS][SRLS] [insufficient-power][invalid-input-current]
[invalid-output-current][member-removed][member-upgrade-notification] [new-master][new-member]
[port-change][power-budget-warning][power-invalid-topology]
[power-link-status-changed][power-oper-status-changed]
[power-priority-conflict][power-version-mismatch][ring-redundant]
[stack-mismatch][unbalanced-power-supplies][under-budget][under-voltage]
```

### Syntax Description

<b>GLS</b>	(Optional) Enables StackWise stack power GLS trap.
<b>ILS</b>	(Optional) Enables StackWise stack power ILS trap.
<b>SRLS</b>	(Optional) Enables StackWise stack power SRLS trap.
<b>insufficient-power</b>	(Optional) Enables StackWise stack power unbalanced power supplies trap.
<b>invalid-input-current</b>	(Optional) Enables StackWise stack power invalid input current trap.
<b>invalid-output-current</b>	(Optional) Enables StackWise stack power invalid output current trap.
<b>member-removed</b>	(Optional) Enables StackWise stack member removed trap.
<b>member-upgrade-notification</b>	(Optional) Enables StackWise member to be reloaded for upgrade trap.
<b>new-master</b>	(Optional) Enables StackWise new master trap.
<b>new-member</b>	(Optional) Enables StackWise stack new member trap.
<b>port-change</b>	(Optional) Enables StackWise stack port change trap.
<b>power-budget-warning</b>	(Optional) Enables StackWise stack power budget warning trap.
<b>power-invalid-topology</b>	(Optional) Enables StackWise stack power invalid topology trap.
<b>power-link-status-changed</b>	(Optional) Enables StackWise stack power link status changed trap.

<b>power-oper-status-changed</b>	(Optional) Enables StackWise stack power port oper status changed trap.
<b>power-priority-conflict</b>	(Optional) Enables StackWise stack power priority conflict trap.
<b>power-version-mismatch</b>	(Optional) Enables StackWise stack power version mismatch discovered trap.
<b>ring-redundant</b>	(Optional) Enables StackWise stack ring redundant trap.
<b>stack-mismatch</b>	(Optional) Enables StackWise stack mismatch trap.
<b>unbalanced-power-supplies</b>	(Optional) Enables StackWise stack power unbalanced power supplies trap.
<b>under-budget</b>	(Optional) Enables StackWise stack power under budget trap.
<b>under-voltage</b>	(Optional) Enables StackWise stack power under voltage trap.

**Command Default** The sending of SNMP StackWise traps is disabled.

**Command Modes** Global configuration

#### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

#### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



**Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

#### Examples

This example shows how to generate StackWise stack power GLS traps:

```
Switch(config)# snmp-server enable traps stackwise GLS
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps storm-control

To enable SNMP storm-control trap parameters, use the **snmp-server enable traps storm-control** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps storm-control** {*trap-rate number-of-minutes*}

**no snmp-server enable traps storm-control** {*trap-rate*}

### Syntax Description

<b>trap-rate</b> <i>number-of-minutes</i>	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000.
---	---

### Command Default

The sending of SNMP storm-control trap parameters is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:

```
Switch(config)# snmp-server enable traps storm-control trap-rate 10
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps stpx [inconsistency][loop-inconsistency][root-inconsistency]
no snmp-server enable traps stpx [inconsistency][loop-inconsistency][root-inconsistency]
```

### Syntax Description

<b>inconsistency</b>	(Optional) Enables SNMP STPX MIB inconsistency update traps.
<b>loop-inconsistency</b>	(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
<b>root-inconsistency</b>	(Optional) Enables SNMP STPX MIB root inconsistency update traps.

### Command Default

The sending of SNMP STPX MIB traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate SNMP STPX MIB inconsistency update traps:

```
Switch(config)# snmp-server enable traps stpx inconsistency
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the **snmp-server enable traps transceiver** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps transceiver** {all}

**no snmp-server enable traps transceiver** {all}

### Syntax Description

**all** (Optional) Enables all SNMP transceiver traps.

### Command Default

The sending of SNMP transceiver traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to set all SNMP transceiver traps:

```
Switch(config)# snmp-server enable traps transceiver all
```

### Related Commands

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

## snmp-server enable traps vstack

To enable SNMP smart install traps, use the **snmp-server enable traps vstack** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**snmp-server enable traps vstack** [**addition**][**failure**][**lost**][**operation**]

**no snmp-server enable traps vstack** [**addition**][**failure**][**lost**][**operation**]

### Syntax Description

<b>addition</b>	(Optional) Enables client added traps.
<b>failure</b>	(Optional) Enables file upload and download failure traps.
<b>lost</b>	(Optional) Enables client lost trap.
<b>operation</b>	(Optional) Enables operation mode change traps.

### Command Default

The sending of SNMP smart install traps is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

### Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



#### Note

Inform traps are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

### Examples

This example shows how to generate SNMP Smart Install client-added traps:

```
Switch(config)# snmp-server enable traps vstack addition
```

**Related Commands**

Command	Description
<a href="#">snmp-server host</a>	Specifies the recipient (host) of a SNMP notification operation.

# snmp-server engineID

To configure a name for either the local or remote copy of SNMP, use the **snmp-server engineID** command in global configuration mode.

**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

## Syntax Description

<b>local</b> <i>engineid-string</i>	Specifies a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value.
<b>remote</b> <i>ip-address</i>	Specifies the remote SNMP copy. Specify the <i>ip-address</i> of the device that contains the remote copy of SNMP.
<b>udp-port</b> <i>port-number</i>	(Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

## Usage Guidelines

None

## Examples

The following example configures a local engine ID of 123400000000000000000000:

```
Switch(config)# snmp-server engineID local 1234
```

## snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the switch. Use the **no** form of this command to remove the specified host.

**snmp-server host** {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} } ] {*community-string* [*notification-type*] }

**no snmp-server host** {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} } ] {*community-string* [*notification-type*] }

### Syntax Description

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
<b>vrf</b> <i>vrf-instance</i>	(Optional) Specifies the virtual private network (VPN) routing instance and name for this host.
<b>informs</b>   <b>traps</b>	(Optional) Sends SNMP traps or informs to this host.
<b>version</b> <b>1</b>   <b>2c</b>   <b>3</b>	(Optional) Specifies the version of the SNMP used to send the traps. <b>1</b> —SNMPv1. This option is not available with informs. <b>2c</b> —SNMPv2C. <b>3</b> —SNMPv3. One of the authorization keywords (see next table row) must follow the Version 3 keyword.
<b>auth</b>   <b>noauth</b>   <b>priv</b>	<b>auth</b> (Optional)—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. <b>noauth</b> (Default)—The noAuthNoPriv security level. This is the default if the <b>auth</b>   <b>noauth</b>   <b>priv</b> keyword choice is not specified. <b>priv</b> (Optional)—Enables Data Encryption Standard (DES) packet encryption (also called privacy).
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string by using the <b>snmp-server host</b> command, we recommend that you define this string by using the <b>snmp-server community</b> global configuration command before using the <b>snmp-server host</b> command.
<b>Note</b>	The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

---

*notification-type* (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:

- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
  - **bridge**—Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.
  - **bulkstat**—Sends Data-Collection-MIB Collection notification traps.
  - **call-home**—Sends SNMP CISCO-CALLHOME-MIB traps.
  - **cef**—Sends SNMP CEF traps.
  - **config**—Sends SNMP configuration traps.
  - **config-copy**—Sends SNMP config-copy traps.
  - **config-ctid**—Sends SNMP config-ctid traps.
  - **copy-config**—Sends SNMP copy configuration traps.
  - **cpu**—Sends CPU notification traps.
  - **cpu threshold**—Sends CPU threshold notification traps.
  - **entity**—Sends SNMP entity traps.
-

- 
- **envmon**—Sends environmental monitor traps.
  - **errdisable**—Sends SNMP errdisable notification traps.
  - **event-manager**—Sends SNMP Embedded Event Manager traps.
  - **flash**—Sends SNMP FLASH notifications.
  - **flowmon**—Sends SNMP flowmon notification traps.
  - **ipmulticast**—Sends SNMP IP multicast routing traps.
  - **ipsla**—Sends SNMP IP SLA traps.
  - **license**—Sends license traps.
  - **local-auth**—Sends SNMP local auth traps.
  - **mac-notification**—Sends SNMP MAC notification traps.
  - **pim**—Sends SNMP Protocol-Independent Multicast (PIM) traps.
  - **power-ethernet**—Sends SNMP power Ethernet traps.
  - **snmp**—Sends SNMP-type traps.
  - **storm-control**—Sends SNMP storm-control traps.
  - **stpx**—Sends SNMP STP extended MIB traps.
  - **syslog**—Sends SNMP syslog traps.
  - **transceiver**—Sends SNMP transceiver traps.
  - **tty**—Sends TCP connection traps.
  - **vlan-membership**—Sends SNMP VLAN membership traps.
  - **vlancreate**—Sends SNMP VLAN-created traps.
  - **vlandelete**—Sends SNMP VLAN-deleted traps.
  - **vrfmib**—Sends SNMP vrfmib traps.
  - **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) traps.
  - **wireless**—Sends wireless traps.
- 

### Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

**Note**

Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

**Command Modes**

Global configuration

**Command History**

Release	Modification
Cisco IOS 15.0(2)EX1	This command was introduced.

**Usage Guidelines**

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

**Examples**

This example shows how to configure a unique SNMP community string named comaccess for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
```

```
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host myhost.cisco.com by using the community string public:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

### Related Commands

Command	Description
snmp-server enable traps	Enables the switch to send SNMP notifications for various traps or inform requests to the NMS.



## INDEX

### D

debug platform ip dhcp command [17](#)  
debug platform snmp command [19](#)

### F

flow-based RSPAN (FRSPAN) session [26](#)  
flow-based SPAN (FSPAN) session [26](#)

### M

monitor session command [20, 22](#)  
monitor session filter command [26](#)  
monitor session source command [28](#)

### R

Remote SPAN (RSPAN) sessions [31](#)  
RSPAN [20, 22, 26, 28](#)  
    sessions [20, 22, 28](#)  
        add interfaces to [20, 22, 28](#)  
        start new [20, 22, 28](#)

### S

show monitor session command [31](#)  
show platform snmp counters command [33](#)  
snmp-server enable traps bridge command [37](#)  
snmp-server enable traps call-home command [38](#)  
snmp-server enable traps cef command [39](#)  
snmp-server enable traps command [34](#)  
snmp-server enable traps CPU command [41](#)  
snmp-server enable traps dot1x command [42](#)  
snmp-server enable traps energywise command [44](#)  
snmp-server enable traps envmon command [46](#)  
snmp-server enable traps errdisable command [48](#)  
snmp-server enable traps flash command [49](#)  
snmp-server enable traps ike command [50](#)  
snmp-server enable traps ipsec command [52](#)  
snmp-server enable traps license command [54](#)  
snmp-server enable traps mac-notification command [55](#)  
snmp-server enable traps ospf command [56](#)  
snmp-server enable traps pim command [58](#)  
snmp-server enable traps port-security command [59](#)  
snmp-server enable traps power-ethernet command [60](#)  
snmp-server enable traps snmp command [61](#)  
snmp-server enable traps stackwise command [63](#)  
snmp-server enable traps storm-control command [66](#)  
snmp-server enable traps stpx command [67](#)  
snmp-server enable traps transceiver command [68](#)  
snmp-server enable traps vstack command [69](#)  
snmp-server engineID command [71](#)  
snmp-server host command [72](#)  
Switched Port Analyzer (SPAN) sessions [31](#)

