



## Preface

---

## Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Catalyst switch, hereafter referred to as *the switch*. Before using this guide, you should have experience working with the Cisco IOS commands and the switch software features. Before using this guide, you should have experience working with the concepts and terminology of Ethernet and local area networking.

## Purpose

This guide provides the information that you need about the Layer 2 commands that have been created or changed for use with the Catalyst switches. For information about the standard Cisco IOS Release 15.0 commands, see the Cisco IOS documentation set available on Cisco.com.

This guide does not provide procedures for configuring your switch. For detailed configuration procedures, see the software configuration guide for this release.

This guide does not describe system messages you might encounter. For more information, see the system message guide for this release.

For documentation updates, see the release notes for this release.

## Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) means optional elements.
- Braces ({{}}) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ({{|}}) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:



**Note**

---

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

---



**Caution**

---

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

---

## Filtering show Command Output

The `show` commands have optional output modifiers to filter the command output.

- `| begin`—Display begins with the line that matches the *expression*.
- `| exclude`—Display excludes with the line that matches the *expression*.
- `| include`—Display includes with the line that matches the *expression*.
- *expression*—Expression in the output to use as a reference point.

Expressions are case sensitive. If you enter `| exclude output`, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Related Publications



**Note**

---

These documents provide complete information about the switch and are available from this Cisco.com site:

Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the “Using Express Setup” section in the getting started guide or the “Configuring the Switch with the CLI-Based Setup Program” appendix in the hardware installation guide.
  - For device manager requirements, see the “System Requirements” section in the release notes (not orderable but available on Cisco.com).
  - For Network Assistant requirements, see the *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com).
  - For cluster requirements, see the *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com).
  - For upgrade information, see the “Downloading Software” section in the release notes.
-

See these documents for other information about the switches:

- *Release Notes for the Catalyst 3750, 3560, 3560-C, 2960, 2960-S, and 2960-C Switches*
- *Catalyst 3750, 3560, 2960, and 2960-S Switch System Message Guide*
- *Auto Smartports Configuration Guide*
- *Call Home Configuration Guide*
- *Cisco EnergyWise Configuration Guide*
- *Smart Install Configuration Guide*
- *Release Notes for Cisco Network Assistant*
- *Getting Started with Cisco Network Assistant*
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide*
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide*
- *Cisco Redundant Power System 2300 Hardware Installation Guide*
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide*.
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:  
[http://www.cisco.com/en/US/products/hw/modules/ps5455/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html)  
These SFP compatibility matrix documents are available from this Cisco.com site:  
[http://www.cisco.com/en/US/products/hw/modules/ps5455/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html)

## Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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



# CHAPTER 1

## Using the Command-Line Interface

---

The Catalyst switch is supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure software features.

- For a complete description of the commands that support these features, see [Chapter 1, “Catalyst 2960-S and 2960-C Switches Cisco IOS Commands.”](#)
- For information on the bootloader commands, see [Appendix 1, “Catalyst Switch Bootloader Commands.”](#)
- For information on the **debug** commands, see [Appendix 1, “Catalyst Switch Debug Commands.”](#)
- For information on the **show platform** commands, see [Appendix 1, “Catalyst Switch Show Platform Commands.”](#)
- For more information on Cisco IOS Release 12.2, see the *Cisco IOS Release 12.2 Command Summary*.
- For task-oriented configuration steps, see the software configuration guide for this release.

In this document, IP refers to IP version 4 (IPv4) unless there is a specific reference to IP version 6 (IPv6).

## CLI Command Modes

This section describes the CLI command mode structure. Command modes support specific Cisco IOS commands. For example, the **interface interface-id** command only works when entered in global configuration mode.

These are the main command modes for the switch:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration
- VLAN configuration
- Line configuration

**Table 1-1** lists the main command modes, how to access each mode, the prompt you see in that mode, and how to exit that mode. The prompts listed use the default name *Switch*.

**Table 1-1 Command Modes Summary**

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User EXEC	This is the first level of access. (For the switch) Change terminal settings, perform basic tasks, and list system information.	Switch>	Enter the <b>logout</b> command. To enter privileged EXEC mode, enter the <b>enable</b> command.
Privileged EXEC	From user EXEC mode, enter the <b>enable</b> command.	Switch#	To exit to user EXEC mode, enter the <b>disable</b> command. To enter global configuration mode, enter the <b>configure</b> command.
Global configuration	From privileged EXEC mode, enter the <b>configure</b> command.	Switch(config)#	To exit to privileged EXEC mode, enter the <b>exit</b> or <b>end</b> command, or press <b>Ctrl-Z</b> . To enter interface configuration mode, enter the <b>interface</b> configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the <b>interface</b> command followed by an interface identification.	Switch(config-if)#	To exit to privileged EXEC mode, enter the <b>end</b> command, or press <b>Ctrl-Z</b> . To exit to global configuration mode, enter the <b>exit</b> command.
VLAN configuration	In global configuration mode, enter the <b>vlan vlan-id</b> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command. To return to privileged EXEC mode, enter the <b>end</b> command, or press <b>Ctrl-Z</b> .
Line configuration	From global configuration mode, specify a line by entering the <b>line</b> command.	Switch(config-line)#	To exit to global configuration mode, enter the <b>exit</b> command. To return to privileged EXEC mode, enter the <b>end</b> command, or press <b>Ctrl-Z</b> .

## User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the user EXEC commands to temporarily change terminal settings, perform basic tests, and list system information.

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (?) at the prompt.

Switch> ?

## Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** privileged EXEC command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

The privileged EXEC mode prompt is the device name followed by the pound sign (#).

```
Switch#
```

Enter the **enable** command to access privileged EXEC mode:

```
Switch> enable  
Switch#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch# ?
```

To return to user EXEC mode, enter the **disable** privileged EXEC command.

## Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console.

When you enter the **configure** command, a message prompts you for the source of the configuration commands:

```
Switch# configure  
Configuring from terminal, memory, or network [terminal]?
```

You can specify either the terminal or NVRAM as the source of configuration commands.

This example shows you how to access global configuration mode:

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(config)# ?
```

To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press **Ctrl-Z**.

## Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the **interface *interface-id*** command to access interface configuration mode. The new prompt means interface configuration mode.

```
Switch(config-if) #
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(config-if) # ?
```

To exit interface configuration mode and to return to global configuration mode, enter the **exit** command. To exit interface configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

## VLAN Configuration Mode

Use this mode to configure normal-range VLANs (VLAN IDs 1 to 1005) or, when VTP mode is transparent, to configure extended-range VLANs (VLAN IDs 1006 to 4094). When VTP mode is transparent, the VLAN and VTP configuration is saved in the running configuration file, and you can save it to the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command. The configurations of VLAN IDs 1 to 1005 are saved in the VLAN database if VTP is in transparent or server mode. The extended-range VLAN configurations are not saved in the VLAN database.

Enter the **vlan *vlan-id*** global configuration command to access config-vlan mode:

```
Switch(config)# vlan 2000
Switch(config-vlan) #
```

The supported keywords can vary but are similar to the commands available in VLAN configuration mode. To display a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(config-vlan) # ?
```

For extended-range VLANs, all characteristics except the MTU size must remain at the default setting.

To return to global configuration mode, enter **exit**; to return to privileged EXEC mode, enter **end**. All the commands except **shutdown** take effect when you exit config-vlan mode.

## Line Configuration Mode

Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. Use these commands to change terminal parameter settings line-by-line or for a range of lines.

Use the **line vty *line\_number* [*ending\_line\_number*]** command to enter line configuration mode. The new prompt means line configuration mode. The following example shows how to enter line configuration mode for virtual terminal line 7:

```
Switch(config)# line vty 0 7
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (?) at the prompt.

```
Switch(config-line)# ?
```

To exit line configuration mode and to return to global configuration mode, use the **exit** command. To exit line configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.



# CHAPTER 1

## Catalyst 2960-S and 2960-C Switches Cisco IOS Commands

### aaa accounting dot1x

Use the **aaa accounting dot1x** global configuration command to enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions. Use the **no** form of this command to disable IEEE 802.1x accounting.

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+} [group {name | radius | tacacs+}...]} | group {name | radius | tacacs+} [group {name | radius | tacacs+}...]
```

```
no aaa accounting dot1x {name | default}
```

Syntax Description	
<b>name</b>	Name of a server group. This is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords.
<b>default</b>	Use the accounting methods that follow as the default list for accounting services.
<b>start-stop</b>	Send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
<b>broadcast</b>	Enable accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
<b>group</b>	Specify the server group to be used for accounting services. These are valid server group names: <ul style="list-style-type: none"><li>• <b>name</b>—Name of a server group.</li><li>• <b>radius</b>—List of all RADIUS hosts.</li><li>• <b>tacacs+</b>—List of all TACACS+ hosts.</li></ul> The <b>group</b> keyword is optional when you enter it after the <b>broadcast group</b> and <b>group</b> keywords. You can enter more than optional <b>group</b> keyword.

---

<b>radius</b>	(Optional) Enable RADIUS authorization.
<b>tacacs+</b>	(Optional) Enable TACACS+ accounting.

---

**Defaults** AAA accounting is disabled.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
------------------------	----------------	---------------------

**Usage Guidelines** This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

**Examples** This example shows how to configure IEEE 802.1x accounting:

 **Note**  
Switch(config)# aaa new-model  
Switch(config)# aaa accounting dot1x default start-stop group radius

The RADIUS authentication server must be properly configured to accept and log update or watchdog packets from the AAA client.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa authentication dot1x</b>	Specifies one or more AAA methods for use on interfaces running IEEE 802.1x.
	<b>aaa new-model</b>	Enables the AAA access control model.
	<b>dot1x reauthentication</b>	Enables or disables periodic reauthentication.
	<b>dot1x timeout reauth-period</b>	Sets the number of seconds between re-authentication attempts.

---

---

 ■ aaa authentication dot1x

## aaa authentication dot1x

Use the **aaa authentication dot1x** global configuration command to specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication. Use the **no** form of this command to disable authentication.

**aaa authentication dot1x {default} method1**

**no aaa authentication dot1x {default}**

<b>Syntax Description</b>	<table border="0"> <tr> <td><b>default</b></td><td>Use the listed authentication method that follows this argument as the default method when a user logs in.</td></tr> <tr> <td><i>method1</i></td><td>Enter the <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.</td></tr> </table>	<b>default</b>	Use the listed authentication method that follows this argument as the default method when a user logs in.	<i>method1</i>	Enter the <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.
<b>default</b>	Use the listed authentication method that follows this argument as the default method when a user logs in.				
<i>method1</i>	Enter the <b>group radius</b> keywords to use the list of all RADIUS servers for authentication.				



**Note** Though other keywords are visible in the command-line help strings, only the **default** and **group radius** keywords are supported.

---

**Defaults** No authentication is performed.

---

**Command Modes** Global configuration

---

### Command History

#### Usage Guidelines

The *method* argument identifies the method that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

---

#### Examples

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

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

**Related Commands**

Command	Description
<b>aaa new-model</b>	Enables the AAA access control model.
<b>show running-config</b>	Displays the current operating configuration.

---

 ■ aaa authorization network

# aaa authorization network

Use the **aaa authorization network** global configuration command to configure the switch to use user-RADIUS authorization for all network-related service requests, such as IEEE 802.1x VLAN assignment. Use the **no** form of this command to disable RADIUS user authorization.

**aaa authorization network default group radius**

**no aaa authorization network default**

---

<b>Syntax Description</b>	<b>default group radius</b>	Use the list of all RADIUS hosts in the server group as the default authorization list.
---------------------------	-----------------------------	---

---

**Defaults** Authorization is disabled.

**Command Modes** Global configuration

---

## Command History

**Usage Guidelines** Use the **aaa authorization network default group radius** global configuration command to allow the switch to download IEEE 802.1x authorization parameters from the RADIUS servers in the default authorization list. The authorization parameters are used by features such as VLAN assignment to get parameters from the RADIUS servers.

Use the **show running-config** privileged EXEC command to display the configured lists of authorization methods.

---

## Examples

This example shows how to configure the switch for user RADIUS authorization for all network-related service requests:

```
Switch(config)# aaa authorization network default group radius
```

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

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show running-config</b>	Displays the current operating configuration.

---

## archive download-sw

Use the **archive download-sw** privileged EXEC command to download a new image from a TFTP server to the switch and to overwrite or keep the existing image.

```
archive download-sw {/directory | /force-reload | /imageonly | /leave-old-sw | /no-set-boot |
/no-version-check | /overwrite | /reload | /safe} source-url
```

Syntax Description	
<b>/directory</b>	Specify a directory for the images.
<b>/force-reload</b>	Unconditionally force a system reload after successfully downloading the software image.
<b>/imageonly</b>	Download only the software image but not the HTML files associated with the embedded device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
<b>/leave-old-sw</b>	Keep the old software version after a successful download.
<b>/no-set-boot</b>	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
<b>/no-version-check</b>	Download the software image without verifying its version compatibility with the image that is running on the switch.
<b>/overwrite</b>	Overwrite the software image in flash memory with the downloaded image.
<b>/reload</b>	Reload the system after successfully downloading the image unless the configuration has been changed and not saved.
<b>/safe</b>	Keep the current software image. Do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.

**archive download-sw**


---

<i>source-url</i>	<p>The source URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> <li>• The syntax for the secondary boot loader (BS1): <b>bs1:</b></li> <li>• The syntax for the local flash file system: <b>flash:</b></li> <li>• The syntax for the FTP: <b>ftp:[//username[:password]@location]/directory]/image-name.tar</b></li> <li>• The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>• The syntax for a secure HTTP server: <b>https://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>• The syntax for the Remote Copy Protocol (RCP): <b>rcp:[//username@location]/directory]/image-name.tar</b></li> <li>• The syntax for the TFTP: <b>tftp:[//location]/directory]/image-name.tar</b></li> </ul> <p>The <b>image-name.tar</b> is the software image to download and install on the switch.</p>
-------------------	---

---

**Defaults**

The current software image is not overwritten with the downloaded image.

Both the software image and HTML files are downloaded.

The new image is downloaded to the flash: file system.

The BOOT environment variable is changed to point to the new software image on the flash: file system.

Image names are case sensitive; the image file is provided in tar format.

**Command Modes**

Privileged EXEC

**Command History****Usage Guidelines**

The **/imageonly** option removes the HTML files for the existing image if the existing image is being removed or replaced. Only the Cisco IOS image (without the HTML files) is downloaded.

Using the **/safe** or **/leave-old-sw** option can cause the new image download to fail if there is insufficient flash memory. If leaving the software in place prevents the new image from fitting in flash memory due to space constraints, an error results.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command. For more information, see the “[delete](#)” section on page 2-129.

Use the **/overwrite** option to overwrite the image on the flash device with the downloaded one.

If you specify the command *without* the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.

After downloading a new image, enter the **reload** privileged EXEC command to begin using the new image, or specify the **/reload** or **/force-reload** option in the **archive download-sw** command.

## Examples

This example shows how to download a new image from a TFTP server at 172.20.129.10 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

This example shows how to keep the old software version after a successful download:

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

## Related Commands

Command	Description
<a href="#">archive tar</a>	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.
<a href="#">archive upload-sw</a>	Uploads an existing image on the switch to a server.
<a href="#">delete</a>	Deletes a file or directory on the flash memory device.

# archive tar

Use the **archive tar** privileged EXEC command to create a tar file, list files in a tar file, or extract the files from a tar file.

```
archive tar {/create destination-url flash:/file-url} |{/table source-url} |{/xtract source-url  
flash:/file-url [dir/file...]}
```

## Syntax Description

<b>/create destination-url flash:/file-url</b>	<p>Create a new tar file on the local or network file system.</p> <p>For <i>destination-url</i>, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:</p> <ul style="list-style-type: none"> <li>• The syntax for the local flash filesystem: <b>flash:</b></li> <li>• The syntax for the FTP: <b>ftp:[//username[:password]@location]/directory]/tar-filename.tar</b></li> <li>• The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}{/directory]/image-name.tar</b></li> <li>• The syntax for a secure HTTP server: <b>https://[[username:password]@]{hostname   host-ip}{/directory]/image-name.tar</b></li> <li>• The syntax for the Remote Copy Protocol (RCP) is: <b>rcp:[//username@location]/directory]/tar-filename.tar</b></li> <li>• The syntax for the TFTP: <b>tftp:[//location]/directory]/tar-filename.tar</b></li> </ul> <p>The <i>tar-filename.tar</i> is the tar file to be created.</p> <p>For <b>flash:/file-url</b>, specify the location on the local flash file system from which the new tar file is created.</p> <p>An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.</p>
--	--

<b>/table</b> <i>source-url</i>	<p>Display the contents of an existing tar file to the screen.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. These options are supported:</p> <ul style="list-style-type: none"> <li>• The syntax for the local flash file system: <b>flash:</b></li> <li>• The syntax for the FTP: <b>ftp:[//username[:password]@location]/directory]/tar-filename.tar</b></li> <li>• The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}{/directory}/image-name.tar</b></li> <li>• The syntax for a secure HTTP server: <b>https://[[username:password]@]{hostname   host-ip}{/directory}/image-name.tar</b></li> <li>• The syntax for the RCP: <b>rcp:[//username@location]/directory]/tar-filename.tar</b></li> <li>• The syntax for the TFTP: <b>tftp:[//location]/directory]/tar-filename.tar</b></li> </ul> <p>The <b>tar-filename.tar</b> is the tar file to display.</p>
<b>/xtract</b> <i>source-url</i> <b>flash:/file-url [dir/file...]</b>	<p>Extract files from a tar file to the local file system.</p> <p>For <i>source-url</i>, specify the source URL alias for the local file system. These options are supported:</p> <ul style="list-style-type: none"> <li>• The syntax for the local flash file system: <b>flash:</b></li> <li>• The syntax for the FTP: <b>ftp:[//username[:password]@location]/directory]/tar-filename.tar</b></li> <li>• The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}{/directory}/image-name.tar</b></li> <li>• The syntax for a secure HTTP server: <b>https://[[username:password]@]{hostname   host-ip}{/directory}/image-name.tar</b></li> <li>• The syntax for the RCP: <b>rcp:[//username@location]/directory]/tar-filename.tar</b></li> <li>• The syntax for the TFTP: <b>tftp:[//location]/directory]/tar-filename.tar</b></li> </ul> <p>The <b>tar-filename.tar</b> is the tar file from which to extract.</p> <p>For <b>flash:/file-url [dir/file...]</b>, specify the location on the local flash file system into which the tar file is extracted. Use the <i>dir/file...</i> option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.</p>

**Defaults**

There is no default setting.

**archive tar****Command Modes** Privileged EXEC**Command History****Usage Guidelines**

Filenames and directory names are case sensitive.

Image names are case sensitive.

**Examples**

This example shows how to create a tar file. The command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

This example shows how to display the contents of the file that is in flash memory. The contents of the tar file appear on the screen:

```
Switch# archive tar /table flash:.tar
info (219 bytes)

/ (directory)
(610856 bytes)
/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the */html* directory and its contents:

```
flash:.tar /html
/html/ (directory)
/html/const.htm (556 bytes)
/html/xhome.htm (9373 bytes)
/html/menu.css (1654 bytes)
<output truncated>
```

This example shows how to extract the contents of a tar file on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">archive download-sw</a>	Downloads a new image from a TFTP server to the switch.
<a href="#">archive upload-sw</a>	Uploads an existing image on the switch to a server.

# archive upload-sw

Use the **archive upload-sw** privileged EXEC command to upload an existing switch image to a server.

**archive upload-sw [/version *version\_string*] destination-url**

<b>Syntax Description</b>	<p><b>/version <i>version_string</i></b> (Optional) Specify the specific version string of the image to be uploaded.</p> <p><b>destination-url</b> The destination URL alias for a local or network file system. These options are supported:</p> <ul style="list-style-type: none"> <li>The syntax for the local flash file system: <b>flash:</b></li> <li>The syntax for the FTP: <b>ftp:[//username[:password]@location]/directory]/image-name.tar</b></li> <li>The syntax for an HTTP server: <b>http://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>The syntax for a secure HTTP server: <b>https://[[username:password]@]{hostname   host-ip}[/directory]/image-name.tar</b></li> <li>The syntax for the Secure Copy Protocol (SCP): <b>scp:[//username@location]/directory]/image-name.tar</b></li> <li>The syntax for the Remote Copy Protocol (RCP): <b>rcp:[//username@location]/directory]/image-name.tar</b></li> <li>The syntax for the TFTP: <b>tftp:[//location]/directory]/image-name.tar</b></li> </ul> <p>The <i>image-name.tar</i> is the name of software image to be stored on the server.</p>
---------------------------	---

<b>Defaults</b>	Uploads the currently running image from the flash file system.
-----------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

### Usage Guidelines

Use the upload feature only if the HTML files associated with the embedded device manager have been installed with the existing image.

The files are uploaded in this sequence: the Cisco IOS image, the HTML files, and info. After these files are uploaded, the software creates the tar file.

Image names are case sensitive.

**archive upload-sw****Examples**

This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-swtftp://172.20.140.2/test-image.tar
```

**Related Commands**

Command	Description
<a href="#">archive download-sw</a>	Downloads a new image to the switch.
<a href="#">archive tar</a>	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.

# arp access-list

Use the **arp access-list** global configuration command to define an Address Resolution Protocol (ARP) access control list (ACL) or to add clauses to the end of a previously defined list. Use the **no** form of this command to delete the specified ARP access list.

**arp access-list acl-name**

**no arp access-list acl-name**

Syntax Description	acl-name	Name of the ACL.
--------------------	----------	------------------

Defaults	No ARP access lists are defined.
----------	----------------------------------

Command Modes	Global configuration
---------------	----------------------

## Command History

### Usage Guidelines

After entering the **arp access-list** command, you enter ARP access-list configuration mode, and these configuration commands are available:

- **default:** returns a command to its default setting.
- **deny:** specifies packets to reject. For more information, see the “[deny \(ARP access-list configuration\)](#)” section on page 2-132.
- **exit:** exits ARP access-list configuration mode.
- **no:** negates a command or returns to default settings.
- **permit:** specifies packets to forward. For more information, see the “[permit \(ARP access-list configuration\)](#)” section on page 2-414.

Use the **permit** and **deny** access-list configuration commands to forward and to drop ARP packets based on the specified matching criteria.

When the ARP ACL is defined, you can apply it to a VLAN by using the **ip arp inspection filter vlan** global configuration command. ARP packets containing only IP-to-MAC address bindings are compared to the ACL. All other types of packets are bridged in the ingress VLAN without validation. If the ACL permits a packet, the switch forwards it. If the ACL denies a packet because of an explicit deny statement, the switch drops the packet. If the ACL denies a packet because of an implicit deny statement, the switch compares the packet to the list of DHCP bindings (unless the ACL is *static*, which means that packets are not compared to the bindings).

### Examples

This example shows how to define an ARP access list and to permit both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 00001.0000.abcd
Switch(config-arp-nacl)# end
```

**■ arp access-list**

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>deny (ARP access-list configuration)</b></a>	Denies an ARP packet based on matches compared against the DHCP bindings.
	<a href="#"><b>ip arp inspection filter vlan</b></a>	Permits ARP requests and responses from a host configured with a static IP address.
	<a href="#"><b>permit (ARP access-list configuration)</b></a>	Permits an ARP packet based on matches compared against the DHCP bindings.
	<a href="#"><b>show arp access-list</b></a>	Displays detailed information about ARP access lists.

# authentication command bounce-port ignore

Use the **authentication command bounce-port ignore** global configuration command on the switch stack or on a standalone switch to allow the switch to ignore a command to temporarily disable a port. Use the **no** form of this command to return to the default status.

**authentication command bounce-port ignore**

**no authentication command bounce-port ignore**

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

**Defaults** The switch accepts a RADIUS Change of Authorization (CoA) **bounce port** command.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** The CoA **bounce port** command causes a link flap, which triggers a DHCP renegotiation from the host. This is useful when a VLAN change occurs and the endpoint is a device such as a printer, that has no supplicant to detect the change. Use this command to configure the switch to ignore the **bounce port** command.

**Examples** This example shows how to instruct the switch to ignore a CoA **bounce port** command:

```
Switch(config)# authentication command bounce-port ignore
```

Related Commands	Command	Description
	<a href="#">authentication command disable-port ignore</a>	Configures the switch to ignore a CoA <b>disable port</b> command.

---

 authentication command disable-port ignore

# authentication command disable-port ignore

Use the **authentication command disable-port ignore** global configuration command on the switch stack or on a standalone switch to allow the switch to ignore a command to disable a port. Use the **no** form of this command to return to the default status.

**authentication command disable-port ignore**

**no authentication command disable-port ignore**

---

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

---

**Defaults** The switch accepts a RADIUS Change of Authorization (CoA) **disable port** command.

---

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

---

**Usage Guidelines** The CoA **disable port** command administratively shuts down a port hosting a session, resulting in session termination. Use this command to configure the switch to ignore this command.

---

**Examples** This example shows how to instruct the switch to ignore a CoA **disable port** command:

```
Switch(config)# authentication command disable-port ignore
```

Related Commands	Command	Description
	<a href="#">authentication command bounce-port ignore</a>	Configures the switch to ignore a CoA <b>bounce port</b> command.

# authentication control-direction

Use the **authentication control-direction** interface configuration command to configure the port mode as unidirectional or bidirectional. Use the **no** form of this command to return to the default setting.

**authentication control-direction {both | in}**

**no authentication control-direction**

<b>Syntax Description</b>	<b>both</b>	Enable bidirectional control on port. The port cannot receive packets from or send packets to the host.
	<b>in</b>	Enable unidirectional control on port. The port can send packets to the host but cannot receive packets from the host.

**Defaults** The port is in bidirectional mode.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Use the **both** keyword or the **no** form of this command to return to the default setting (bidirectional mode).

**Examples** This example shows how to enable bidirectional mode:

```
Switch(config-if)# authentication control-direction both
```

This example shows how to enable unidirectional mode:

```
Switch(config-if)# authentication control-direction in
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
	<b>authentication open</b>	Enables or disables open access on a port.
	<b>authentication order</b>	Sets the order of authentication methods used on a port.

**■ authentication control-direction**

<b>Command</b>	<b>Description</b>
<b>authentication periodic</b>	Enable or disables reauthentication on a port.
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication event

To set the actions for specific authentication events on the port, use the **authentication event** interface configuration command. To return to the default settings, use the **no** form of the command.

```
authentication event {fail [retry retry count] action {authorize vlan vlan-id | next-method} | {no-response action authorize vlan vlan-id} | {server {alive action reinitialize} | {dead action {authorize {vlan vlan-id | voice} | reinitialize vlan}}}}
no authentication event {fail | no-response | {server {alive} | {dead [action {authorize {vlan vlan-id | voice} | reinitialize vlan}}]}}
```

Syntax Description	
<b>action</b>	Configures the required action for an authentication event.
<b>alive</b>	Configures the authentication, authorization, and accounting (AAA) server alive actions.
<b>authorize</b>	Authorizes the VLAN on the port.
<b>dead</b>	Configures the AAA server dead actions.
<b>fail</b>	Configures the failed-authentication parameters.
<b>next-method</b>	Moves to next authentication method.
<b>no-response</b>	Configures the nonresponsive host actions.
<b>reinitialize</b>	Reinitializes all authorized clients.
<b>retry</b>	Enables retry attempts after a failed authentication.
<i>retry count</i>	Number of retry attempts from 0 to 5.
<b>server</b>	Configures the actions for AAA server events.
<b>vlan</b>	Specifies the authentication-fail VLAN.
<i>vlan-id</i>	VLAN ID number from 1 to 4094.
<b>voice</b>	Specifies that if the traffic from the host is tagged with the voice VLAN, the device is placed in the configured voice VLAN on the port.

Defaults	No event responses are configured on the port.
----------	--

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.2(50)SE	This command was introduced.
	12.2(52)SE	The <b>reinitialize</b> keyword was added.
	12.2(53)SE2	This command was introduced.
	15.0(1)SE	The <b>voice</b> keyword was added.

**Usage Guidelines**

Use this command with the **fail**, **no-response**, or **event** keywords to configure the switch response for a specific action.

For *authentication-fail* events:

- If the supplicant fails authentication, the port is moved to a restricted VLAN, and an EAP success message is sent to the supplicant because it is not notified of the actual authentication failure.
  - If the EAP success message is not sent, the supplicant tries to authenticate every 60 seconds (the default) by sending an EAP-start message.
  - Some hosts (for example, devices running Windows XP) cannot implement DHCP until they receive an EAP success message.

The restricted VLAN is supported only in single host mode (the default port mode). When a port is placed in a restricted VLAN, the supplicant MAC address is added to the MAC address table. Any other MAC address on the port is treated as a security violation.

- You cannot configure an internal VLAN for Layer 3 ports as a restricted VLAN. You cannot specify the same VLAN as a restricted VLAN and as a voice VLAN.

Enable re-authentication with restricted VLANs. If re-authentication is disabled, the ports in the restricted VLANs do not receive re-authentication requests.

To start the re-authentication process, the restricted VLAN must receive a link-down event or an Extensible Authentication Protocol (EAP) logoff event from the port. If a host is connected through a hub:

- The port might not receive a link-down event when the host is disconnected.
- The port might not detect new hosts until the next re-authentication attempt occurs.

When you reconfigure a restricted VLAN as a different type of VLAN, ports in the restricted VLAN are also moved and stay in their currently authorized state.

For *no-response* events:

- If you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.
- The switch maintains the EAPOL packet history. If another EAPOL packet is detected on the port during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is cleared.
- If the switch port is moved to the guest VLAN (multihost mode), multiple non-IEEE 802.1x-capable clients are allowed access. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put in the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication restarts.

You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN, a primary private VLAN, or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is supported only on access ports. It is not supported on internal VLANs (routed ports) or trunk ports.

- When MAC authentication bypass is enabled on an IEEE 802.1x port, the switch can authorize clients based on the client MAC address if IEEE 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an IEEE 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address.
  - If authorization succeeds, the switch grants the client access to the network.

- If authorization fails, the switch assigns the port to the guest VLAN if one is specified.

For more information, see the "Using IEEE 802.1x Authentication with MAC Authentication Bypass" section in the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the software configuration guide.

For *server-dead* events:

- When the switch moves to the critical-authentication state, new hosts trying to authenticate are moved to the critical-authentication VLAN (or *critical VLAN*). This applies whether the port is in single-host, multiple-host, multi-auth, or MDA mode. Authenticated hosts remain in the authenticated VLAN, and the reauthentication timers are disabled.
- If a client is running Windows XP and the critical port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
- If the Windows XP client is configured for DHCP and has an IP address from the DHCP server and a critical port receives an EAP-Success message, the DHCP configuration process might not re-initiate.

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

## Examples

This example shows how to configure the **authentication event fail** command:

```
Switch(config-if)# authentication event fail action authorize vlan 20
```

This example shows how to configure a no-response action:

```
Switch(config-if)# authentication event no-response action authorize vlan 10
```

This example shows how to configure a server-response action:

```
Switch(config-if)# authentication event server alive action reinitialize
```

This example shows how to configure a port to send both new and existing hosts to the critical VLAN when the RADIUS server is unavailable. Use this command for ports in multiple authentication (multi-auth) mode or if the voice domain of the port is in MDA mode:

```
Switch(config-if)# authentication event server dead action authorize vlan 10
```

This example shows how to configure a port to send both new and existing hosts to the critical VLAN when the RADIUS server is unavailable and if the traffic from the host is tagged with the voice VLAN to put the host in the configured voice VLAN on the port. Use this command for ports in multiple-host or multiauth mode:

```
Switch(config-if)# authentication event server dead action reinitialize vlan 10
Switch(config-if)# authentication event server dead action authorize voice
```

## Related Commands

Command	Description
<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
<b>authentication open</b>	Enables or disables open access on a port.
<b>authentication order</b>	Sets the order of authentication methods used on a port.

**■ authentication event**

<b>Command</b>	<b>Description</b>
<b>authentication periodic</b>	Enables or disables reauthentication on a port.
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication fallback

Use the **authentication fallback** interface configuration command to configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. To return to the default setting, use the **no** form of this command.

**authentication fallback *name***

**no authentication fallback *name***

<b>Syntax Description</b>	<i>name</i>	Specify a web authentication fallback profile.
---------------------------	-------------	--

<b>Defaults</b>	No fallback is enabled.
-----------------	-------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	You must enter the <b>authentication port-control auto</b> interface configuration command before configuring a fallback method.
-------------------------	--

You can only configure web authentication as a fallback method to 802.1x or MAB, so one or both of these authentication methods should be configured for the fallback to enable.

<b>Examples</b>	This example shows how to specify a fallback profile on a port:
-----------------	---

```
Switch(config-if)# authentication fallback profile1
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
	<b>authentication open</b>	Enables or disable open access on a port.
	<b>authentication order</b>	Sets the order of authentication methods used on a port.
	<b>authentication periodic</b>	Enables or disables reauthentication on a port.

**■ authentication fallback**

<b>Command</b>	<b>Description</b>
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication host-mode

Use the **authentication host-mode** interface configuration command to set the authorization manager mode on a port.

**authentication host-mode [multi-auth | multi-domain | multi-host | single-host]**

**no authentication host-mode [multi-auth | multi-domain | multi-host | single-host]**

Syntax Description	<b>multi-auth</b> Enable multiple-authorization mode (multiauth mode) on the port.
	<b>multi-domain</b> Enable multiple-domain mode on the port.
	<b>multi-host</b> Enable multiple-host mode on the port.
	<b>single-host</b> Enable single-host mode on the port.

**Defaults** Single host mode is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP Phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

**Examples** This example shows how to enable **multiauth** mode on a port:

```
Switch(config-if)# authentication host-mode multi-auth
```

This example shows how to enable **multi-domain** mode on a port:

```
Switch(config-if)# authentication host-mode multi-domain
```

This example shows how to enable **multi-host** mode on a port:

```
Switch(config)# authentication host-mode multi-host
```

**■ authentication host-mode**

This example shows how to enable **single-host** mode on a port:

```
Switch(config-if)# authentication host-mode single-host
```

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

Related Commands	Command	Description
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication
	<b>authentication open</b>	Enables or disable open access on a port.
	<b>authentication order</b>	Sets the order of authentication methods used on a port.
	<b>authentication periodic</b>	Enables or disable reauthentication on a port.
	<b>authentication port-control</b>	Enables manual control of the port authorization state.
	<b>authentication priority</b>	Adds an authentication method to the port-priority list.
	<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
	<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
	<b>show authentication</b>	Displays information about authentication manager events on the switch.

**Note**


---

# authentication mac-move permit

Use the **authentication mac-move permit** global configuration command to enable MAC move on a switch. Use the **no** form of this command to return to the default setting.

**authentication mac-move permit**

**no authentication mac-move permit**

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

**Defaults** MAC move is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** The command enables authenticated hosts to move between 802.1x-enabled ports on a switch. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated.

MAC move is not supported on port-security enabled 802.1x ports. If MAC move is globally configured on the switch and a port security-enabled host moves to an 802.1x-enabled port, a violation error occurs.

**Examples** This example shows how to enable MAC move on a switch:

```
Switch(config)# authentication mac-move permit
```

Related Commands	Command	Description
	<a href="#">authentication event</a>	Sets the action for specific authentication events.
	<a href="#">authentication fallback</a>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<a href="#">authentication host-mode</a>	Sets the authorization manager mode on a port.
	<a href="#">authentication open</a>	Enables or disables open access on a port.
	<a href="#">authentication order</a>	Sets the order of authentication methods used on a port.
	<a href="#">authentication periodic</a>	Enable or disables reauthentication on a port.

■ authentication mac-move permit

Command	Description
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication open

Use the **authentication open** interface configuration command to enable or disable open access on a port. Use the **no** form of this command to disable open access.

**authentication open**

**no authentication open**

**Defaults** Open access is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Open authentication must be enabled if a device requires network access before it is authenticated. A port ACL should be used to restrict host access when open authentication is enabled.

**Examples** This example shows how to enable open access on a port:

```
Switch(config-if)# authentication open
```

This example shows how to set the port to disable open access on a port:

```
Switch(config-if)# no authentication open
```

Related Commands	Command	Description
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
	<b>authentication order</b>	Sets the order of authentication methods used on a port.
	<b>authentication periodic</b>	Enables or disables reauthentication on a port.
	<b>authentication port-control</b>	Enables manual control of the port authorization state.
	<b>authentication priority</b>	Adds an authentication method to the port-priority list.

**■ authentication open**

Command	Description
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication order

Use the **authentication order** interface configuration command to set the order of authentication methods used on a port.

**authentication order [dot1x | mab] {webauth}**

**no authentication order**

<b>Syntax Description</b>	<b>dot1x</b> Add 802.1x to the order of authentication methods. <b>mab</b> Add MAC authentication bypass (MAB) to the order of authentication methods. <b>webauth</b> Add web authentication to the order of authentication methods.
---------------------------	--

**Command Default** The default authentication order is **dot1x** followed by **mab** and **webauth**.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Ordering sets the order of methods that the switch attempts when trying to authenticate a new device connected to a port. If one method in the list is unsuccessful, the next method is attempted. Each method can only be entered once. Flexible ordering is only possible between 802.1x and MAB. Web authentication can be configured as either a standalone method or as the last method in the order after either 802.1x or MAB. Web authentication should be configured only as fallback to **dot1x** or **mab**.

**Examples** This example shows how to add 802.1x as the first authentication method, MAB as the second method, and web authentication as the third method:

```
Switch(config-if)# authentication order dot1x mab webauth
```

This example shows how to add MAC authentication Bypass (MAB) as the first authentication method and web authentication as the second authentication method:

```
Switch(config-if)# authentication order mab webauth
```

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

**■ authentication order**

Related Commands	Command	Description
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
	<b>authentication open</b>	Enables or disables open access on a port.
	<b>authentication periodic</b>	Enables or disables reauthentication on a port.
	<b>authentication port-control</b>	Enables manual control of the port authorization state.
	<b>authentication priority</b>	Adds an authentication method to the port-priority list.
	<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
	<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
	<b>mab</b>	Enables MAC authentication bypass on a port.
	<b>mab eap</b>	Configures a port to use Extensible Authentication Protocol (EAP).
	<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication periodic

Use the **authentication periodic** interface configuration command to enable or disable reauthentication on a port. Enter the **no** form of this command to disable reauthentication.

**authentication periodic**

**no authentication periodic**

**Command Default** Reauthentication is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** You configure the amount of time between periodic re-authentication attempts by using the **authentication timer reauthentication** interface configuration command.

**Examples** This example shows how to enable periodic reauthentication on a port:

```
Switch(config-if)# authentication periodic
```

This example shows how to disable periodic reauthentication on a port:

```
Switch(config-if)# no authentication periodic
```

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

Related Commands	Command	Description
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
	<b>authentication open</b>	Enables or disable open access on a port.
	<b>authentication order</b>	Sets the order of authentication methods used on a port.
	<b>authentication port-control</b>	Enables manual control of the port authorization state.
	<b>authentication priority</b>	Adds an authentication method to the port-priority list.

**■ authentication periodic**

Command	Description
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication port-control

Use the **authentication port-control** interface configuration command to enable manual control of the port authorization state. Use the **no** form of this command to return to the default setting.

**authentication port-control {auto | force-authorized | force-un authorized}**

**no authentication port-control {auto | force-authorized | force-un authorized}**

<b>Syntax Description</b>	<b>auto</b> Enable IEEE 802.1x authentication on the port. The port changes to the authorized or unauthorized state based, on the IEEE 802.1x authentication exchange between the switch and the client. <b>force-authorized</b> Disable IEEE 802.1x authentication on the port. The port changes to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client. <b>force-un authorized</b> Deny all access the port. The port changes to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.
---------------------------	--

**Defaults** The default setting is force-authorized.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Use the **auto** keyword only on one of these port types:

- Trunk port—if you try to enable IEEE 802.1x authentication on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.
- Dynamic ports—a dynamic port can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x authentication on a dynamic port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, an error message appears, and the port mode does not change.
- Dynamic-access ports—if you try to enable IEEE 802.1x authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN, an error message appears, and the VLAN configuration does not change.

**authentication port-control**

- EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—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 or RSPAN destination. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

To globally disable IEEE 802.1x authentication on the switch, use the **no dot1x system-auth-control** global configuration command. To disable IEEE 802.1x authentication on a specific port or to return to the default setting, use the **no authentication port-control** interface configuration command.

**Examples**

This example shows how to set the port state to automatic:

```
Switch(config-if)# authentication port-control auto
```

This example shows how to set the port state to the force-authorized state:

```
Switch(config-if)# authentication port-control force-authorized
```

This example shows how to set the port state to the force-unauthorized state:

```
Switch(config-if)# authentication port-control force-unauthorized
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">authentication control-direction</a>	Configures the port mode as unidirectional or bidirectional.
<a href="#">authentication event</a>	Sets the action for specific authentication events.
<a href="#">authentication fallback</a>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<a href="#">authentication host-mode</a>	Sets the authorization manager mode on a port.
<a href="#">authentication open</a>	Enables or disables open access on a port.
<a href="#">authentication order</a>	Sets the order of the authentication methods used on a port.
<a href="#">authentication periodic</a>	Enables or disable reauthentication on a port.
<a href="#">authentication priority</a>	Adds an authentication method to the port-priority list.
<a href="#">authentication timer</a>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<a href="#">authentication violation</a>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<a href="#">show authentication</a>	Displays information about authentication manager events on the switch.

# authentication priority

Use the **authentication priority** interface configuration command to add an authentication method to the port-priority list.

**auth priority [dot1x | mab] {webauth}**

**no auth priority [dot1x | mab] {webauth}**

<b>Syntax Description</b>	<b>dot1x</b> Add 802.1x to the order of authentication methods. <b>mab</b> Add MAC authentication bypass (MAB) to the order of authentication methods. <b>webauth</b> Add web authentication to the order of authentication methods.
---------------------------	--

<b>Command Default</b>	The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.
------------------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.  When configuring multiple fallback methods on a port, set web authentication (webauth) last.  Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.
-------------------------	---



<b>Note</b>	If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.
-------------	--

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass, and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

**■ authentication priority****Examples**

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Switch(config-if)# authentication priority dotx webauth
```

This example shows how to set MAC authentication Bypass (MAB) as the first authentication method and web authentication as the second authentication method:

```
Switch(config-if)# authentication priority mab webauth
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">authentication control-direction</a>	Configures the port mode as unidirectional or bidirectional.
<a href="#">authentication event</a>	Sets the action for specific authentication events.
<a href="#">authentication fallback</a>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<a href="#">authentication host-mode</a>	Sets the authorization manager mode on a port.
<a href="#">authentication open</a>	Enables or disables open access on a port.
<a href="#">authentication order</a>	Sets the order of authentication methods used on a port.
<a href="#">authentication periodic</a>	Enables or disables reauthentication on a port.
<a href="#">authentication port-control</a>	Enables manual control of the port authorization state.
<a href="#">authentication timer</a>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<a href="#">authentication violation</a>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<a href="#">mab</a>	Enables MAC authentication bypass on a port.
<a href="#">mab eap</a>	Configures a port to use Extensible Authentication Protocol (EAP).
<a href="#">show authentication</a>	Displays information about authentication manager events on the switch.

# authentication timer

Use the **authentication timer** interface configuration command to configure the timeout and reauthentication parameters for an 802.1x-enabled port.

```
authentication timer {{[inactivity | reauthenticate] [server | am]} {restart value}}
```

```
no authentication timer {{[inactivity | reauthenticate] [server | am]} {restart value}}
```

<b>Syntax Description</b>	<table border="1"> <tr> <td><b>inactivity</b></td><td>Interval in seconds after which the client is unauthorized if there is no activity.</td></tr> <tr> <td><b>reauthenticate</b></td><td>Time in seconds after which an automatic re-authentication attempt starts.</td></tr> <tr> <td><b>server</b></td><td>Interval in seconds after which an attempt is made to authenticate an unauthorized port.</td></tr> <tr> <td><b>restart</b></td><td>Interval in seconds after which an attempt is made to authenticate an unauthorized port.</td></tr> <tr> <td><b>value</b></td><td>Enter a value between 1 and 65535 (in seconds).</td></tr> </table>	<b>inactivity</b>	Interval in seconds after which the client is unauthorized if there is no activity.	<b>reauthenticate</b>	Time in seconds after which an automatic re-authentication attempt starts.	<b>server</b>	Interval in seconds after which an attempt is made to authenticate an unauthorized port.	<b>restart</b>	Interval in seconds after which an attempt is made to authenticate an unauthorized port.	<b>value</b>	Enter a value between 1 and 65535 (in seconds).
<b>inactivity</b>	Interval in seconds after which the client is unauthorized if there is no activity.										
<b>reauthenticate</b>	Time in seconds after which an automatic re-authentication attempt starts.										
<b>server</b>	Interval in seconds after which an attempt is made to authenticate an unauthorized port.										
<b>restart</b>	Interval in seconds after which an attempt is made to authenticate an unauthorized port.										
<b>value</b>	Enter a value between 1 and 65535 (in seconds).										

**Defaults** The **inactivity**, **server**, and **restart** keywords are set to 60 seconds. The **reauthenticate** keyword is set to one hour.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

**Usage Guidelines** If a timeout value is not configured, an 802.1x session stays authorized indefinitely. No other host can use the port, and the connected host cannot move to another port on the same switch.

**Examples** This example shows how to set the authentication inactivity timer to 60 seconds:

```
Switch(config-if)# authentication timer inactivity 60
```

This example shows how to set the reauthentication timer to 120 seconds:

```
Switch(config-if)# authentication timer restart 120
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.

**■ authentication timer**

<b>Command</b>	<b>Description</b>
<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
<b>authentication open</b>	Enables or disables open access on a port.
<b>authentication order</b>	Sets the order of authentication methods used on a port.
<b>authentication periodic</b>	Enables or disables reauthentication on a port.
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
<b>show authentication</b>	Displays information about authentication manager events on the switch.

# authentication violation

Use the **authentication violation** interface configuration command to configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.

**authentication violation {protect | replace | restrict | shutdown}**

**no authentication violation {protect | replace | restrict | shutdown}**

Syntax Description	<b>protect</b> Unexpected incoming MAC addresses are dropped. No syslog errors are generated.
	<b>replace</b> Removes the current session and initiates authentication with the new host.
	<b>restrict</b> Generates a syslog error when a violation error occurs.
	<b>shutdown</b> Error disables the port or the virtual port on which an unexpected MAC address occurs.

**Defaults** By default **authentication violation shutdown** mode is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(50)SE	This command was introduced.
	12.2(55)SE	The <b>replace</b> keyword was added.

**Examples** This example shows how to configure an IEEE 802.1x-enabled port as error disabled and to shut down when a new device connects it:

```
Switch(config-if)# authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Switch(config-if)# authentication violation restrict
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Switch(config-if)# authentication violation protect
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Switch(config-if)# authentication violation replace
```

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

■ authentication violation

Related Commands	Command	Description
	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.
	<b>authentication event</b>	Sets the action for specific authentication events.
	<b>authentication fallback</b>	Configures a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.
	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.
	<b>authentication open</b>	Enables or disables open access on a port.
	<b>authentication order</b>	Sets the order of authentication methods used on a port.
	<b>authentication periodic</b>	Enables or disables reauthentication on a port.
	<b>authentication port-control</b>	Enables manual control of the port authorization state.
	<b>authentication priority</b>	Adds an authentication method to the port-priority list.
	<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
	<b>show authentication</b>	Displays information about authentication manager events on the switch.

# auto qos classify

Use the **auto qos classify** interface configuration command to automatically configure quality of service (QoS) classification for untrusted devices within a QoS domain. Use the **no** form of this command to return to the default setting.

**auto qos classify [police]**

**no auto qos classify [police]**

Syntax Description	police (Optional) Configure QoS policing for untrusted devices.
--------------------	--

## Defaults

Auto-QoS classify is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues

**Table 1-1 Auto-QoS Configuration for the Ingress Queues**

Ingress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
SRR <sup>1</sup> shared	1	0, 1, 2, 3, 6, 7	70 percent	90 percent
Priority	2	4, 5	30 percent	10 percent

1. SRR = shaped round robin. Ingress queues support shared mode only.

[Table 2-2](#) shows the generated auto-QoS configuration for the egress queues.

**Table 1-2 Auto-QoS Configuration for the Egress Queues**

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**auto qos classify****Usage Guidelines**

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the switch for connectivity with a trusted interface. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packets is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

This is the policy map when the **auto qos classify** command is configured:

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
class AUTOQOS_MULTIENHANCED_CONF_CLASS
set dscp af41
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
class AUTOQOS_DEFAULT_CLASS
set dscp default
```

This is the policy map when the **auto qos classify police** command is configured:

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
class AUTOQOS_MULTIENHANCED_CONF_CLASS
set dscp af41
police 5000000 8000 exceed-action drop
class AUTOQOS_BULK_DATA_CLASS
set dscp af11
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_TRANSACTION_CLASS
set dscp af21
police 10000000 8000 exceed-action policed-dscp-transmit
class AUTOQOS_SCAVANGER_CLASS
set dscp cs1
police 10000000 8000 exceed-action drop
class AUTOQOS_SIGNALING_CLASS
set dscp cs3
police 32000 8000 exceed-action drop
class AUTOQOS_DEFAULT_CLASS
set dscp default
police 10000000 8000 exceed-action policed-dscp-transmit
```

**Note**

The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging. For more information, see the **debug auto qos** command.

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified. The CoS, DSCP, and IP precedence values in the packet are not changed. Traffic is switched in pass-through mode. Packets are switched without any rewrites and classified as best effort without any policing.

**Examples**

This example shows how to enable auto-QoS classification of an untrusted device and police traffic:

```
Switch(config-if)# auto qos classify police
```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>debug auto qos</b></a>	Enables debugging of the auto-QoS feature.
<a href="#"><b>mls qos trust</b></a>	Configures the port trust state.
<a href="#"><b>srr-queue bandwidth share</b></a>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.
<a href="#"><b>queue-set</b></a>	Maps a port to a queue-set.
<a href="#"><b>show auto qos</b></a>	Displays auto-QoS information.
<a href="#"><b>show mls qos interface</b></a>	Displays QoS information at the port level.

**auto qos trust**

# auto qos trust

Use the **auto qos trust** interface configuration command on the switch stack or on a standalone switch to automatically configure quality of service (QoS) for trusted interfaces within a QoS domain. Use the **no** form of this command to return to the default setting.

**auto qos trust {cos | dscp}**

**no auto qos trust {cos | dscp}**

<b>Syntax Description</b>	<b>cos</b> Trust the CoS packet classification. <b>dscp</b> Trust the DSCP packet classification.
---------------------------	--

<b>Defaults</b>	Auto-QoS trust is disabled on the port. When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.
-----------------	---

**Table 1-3 Traffic Types, Packet Labels, and Queues**

	<b>VOIP Data Traffic</b>	<b>VOIP Control Traffic</b>	<b>Routing Protocol Traffic</b>	<b>STP<sup>1</sup> BPDU<sup>2</sup> Traffic</b>	<b>Real-Time Video Traffic</b>	<b>All Other Traffic</b>
DSFP <sup>3</sup>	46	24, 26	48	56	34	—
CoS <sup>4</sup>	5	3	6	7	3	—
CoS-to-ingress queue map	4, 5 (queue 2)					0, 1, 2, 3, 6, 7(queue 1)
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)		0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

1. STP = Spanning Tree Protocol

2. BPDU = bridge protocol data unit

3. DSCP = Differentiated Services Code Point

4. CoS = class of service

**Table 1-4 Auto-QoS Configuration for the Ingress Queues**

<b>Ingress Queue</b>	<b>Queue Number</b>	<b>CoS-to-Queue Map</b>	<b>Queue Weight (Bandwidth)</b>	<b>Queue (Buffer) Size</b>
SRR <sup>1</sup> shared	1	0, 1, 2, 3 ,6, 7	70 percent	90 percent
Priority	2	4, 5	30 percent	10 percent

1. SRR = shaped round robin. Ingress queues support shared mode only.

**Table 1-5 Auto-QoS Configuration for the Egress Queues**

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the switch for connectivity with a trusted interface. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packets is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

If the port is configured with auto-QoS trust, it trusts all the packets on the port. If the packets are not marked with a DSCP or CoS value, default marking takes affect.



The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging. For more information, see the **debug auto qos** command.

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered

**auto qos trust**

disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

**Examples**

This example shows how to enable auto-QoS for a trusted interface with specific cos classification.

```
Switch(config)# interface
Switch(config-if)# auto qos trust cos
```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>debug auto qos</b></a>	Enables debugging of the auto-QoS feature.
<a href="#"><b>mls qos trust</b></a>	Configures the port trust state.
<a href="#"><b>srr-queue bandwidth share</b></a>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.
<a href="#"><b>queue-set</b></a>	Maps a port to a queue-set.
<a href="#"><b>show auto qos</b></a>	Displays auto-QoS information.
<a href="#"><b>show mls qos interface</b></a>	Displays QoS information at the port level.

# auto qos video

Use the **auto qos video** interface configuration command on the switch stack or on a standalone switch to automatically configure quality of service (QoS) for video within a QoS domain. Use the **no** form of this command to return to the default setting.

**auto qos video {cts | ip-camera}**

**no auto qos video {cts | ip-camera}**

<b>Syntax Description</b>	<b>cts</b>	Identify this port as connected to a Cisco TelePresence System and automatically configure QoS for video.
	<b>ip-camera</b>	Identify this port as connected to a Cisco IP camera and automatically configure QoS for video.

## Defaults

Auto-QoS video is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

**Table 1-6 Traffic Types, Packet Labels, and Queues**

	<b>VOIP Data Traffic</b>	<b>VOIP Control Traffic</b>	<b>Routing Protocol Traffic</b>	<b>STP<sup>1</sup> BPDU<sup>2</sup> Traffic</b>	<b>Real-Time Video Traffic</b>	<b>All Other Traffic</b>
DSCP <sup>3</sup>	46	24, 26	48	56	34	—
CoS <sup>4</sup>	5	3	6	7	3	—
CoS-to-ingress queue map	4, 5 (queue 2)					0, 1, 2, 3, 6, 7(queue 1)
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)			0 (queue 3)	2 (queue 3) 0, 1 (queue 4)

1. STP = Spanning Tree Protocol

2. BPDU = bridge protocol data unit

3. DSCP = Differentiated Services Code Point

4. CoS = class of service

**Table 1-7 Auto-QoS Configuration for the Ingress Queues**

<b>Ingress Queue</b>	<b>Queue Number</b>	<b>CoS-to-Queue Map</b>	<b>Queue Weight (Bandwidth)</b>	<b>Queue (Buffer) Size</b>
SRR <sup>1</sup> shared	1	0, 1, 2, 3, 6, 7	70 percent	90 percent
Priority	2	4, 5	30 percent	10 percent

1. SRR = shaped round robin. Ingress queues support shared mode only.

**Table 1-8** Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** Use this command to configure the QoS appropriate for video traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the switch for video connectivity with a Cisco TelePresence system and a Cisco IP camera.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.



**Note**

The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging. For more information, see the **debug auto qos** command.

To disable auto-QoS on a port, use the **no auto qos video** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos video** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

## Examples

This example shows how to enable auto-QoS for a Cisco Telepresence interface with conditional trust. The interface is trusted only if a Cisco Telepresence device is detected; otherwise, the port is untrusted.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos video cts
```

You can verify your settings by entering the **show auto qos video interface *interface-id*** privileged EXEC command.

## Related Commands

Command	Description
<b>debug auto qos</b>	Enables debugging of the auto-QoS feature.
<b>mls qos trust</b>	Configures the port trust state.
<b>srr-queue bandwidth share</b>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.
<b>queue-set</b>	Maps a port to a queue-set.
<b>show auto qos</b>	Displays auto-QoS information.
<b>show mls qos interface</b>	Displays QoS information at the port level.

**auto qos voip**

## auto qos voip

Use the **auto qos voip** interface configuration command to automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain. Use the **no** form of this command to return to the default setting.

**auto qos voip {cisco-phone | cisco-softphone | trust}**

**no auto qos voip [cisco-phone | cisco-softphone | trust]**

<b>Syntax Description</b>	<b>cisco-phone</b>	Identify this port as connected to a Cisco IP Phone, and automatically configure QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
	<b>cisco-softphone</b>	Identify this port as connected to a device running the Cisco SoftPhone, and automatically configure QoS for VoIP.
	<b>trust</b>	Identify this port as connected to a trusted switch or router, and automatically configure QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted.

**Defaults** When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

**Table 1-9 Traffic Types, Packet Labels, and Queues**

	<b>VOIP Data Traffic</b>	<b>VOIP Control Traffic</b>	<b>Routing Protocol Traffic</b>	<b>STP<sup>1</sup> BPDU<sup>2</sup> Traffic</b>	<b>Real-Time Video Traffic</b>	<b>All Other Traffic</b>
DSVP <sup>3</sup>	46	24, 26	48	56	34	—
CoS <sup>4</sup>	5	3	6	7	3	—
CoS-to-ingress queue map	4, 5 (queue 2)					0, 1, 2, 3, 6, 7(queue 1)
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)		0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

1. STP = Spanning Tree Protocol

2. BPDU = bridge protocol data unit

3. DSVP = Differentiated Services Code Point

4. CoS = class of service

**Table 1-10 Auto-QoS Configuration for the Ingress Queues**

Ingress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
SRR <sup>1</sup> shared	1	0, 1, 2, 3, 6, 7	70 percent	90 percent
Priority	2	4, 5	30 percent	10 percent

1. SRR = shaped round robin. Ingress queues support shared mode only.

**Table 1-11 Auto-QoS Configuration for the Egress Queues**

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(55)SE	Support for enhanced auto-QoS was added.

**Usage Guidelines** Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the switch, the interior of the network, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the switch for VoIP with Cisco IP Phones on switch and routed ports and for VoIP with devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

The **show auto qos** command output shows the service policy information for the Cisco IP phone.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.



**Note** The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

**auto qos voip**

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.
- When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP Phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP Phone. When a Cisco IP Phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. The switch also uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The switch configures ingress and egress queues on the port according to the settings in [Table 2-10](#) and [Table 2-11](#). The policing is applied to traffic matching the policy-map classification before the switch enables the trust boundary feature.

If the switch port was configured by using the **auto qos voip cisco-phone** interface configuration command in Cisco IOS Release 12.2(37)SE or earlier, the auto-QoS generated commands new to Cisco IOS Release 12.2(40)SE are not applied to the port. To have these commands automatically applied, you must remove and then reapply the configuration to the port.

- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. The switch configures ingress and egress queues on the port according to the settings in [Table 2-10](#) and [Table 2-11](#).
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the interior of the network, the switch trusts the CoS value for nonrouted ports in ingress packets (the assumption is that traffic has already been classified by other edge devices). The switch configures the ingress and egress queues on the port according to the settings in [Table 2-10](#) and [Table 2-11](#).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.



**Note** When a device running Cisco SoftPhone is connected to a switch or routed port, the switch supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered

disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

On a port on which the **auto qos voip** command is enabled, the queue-set ID that is generated depends on the interface:

- For a Fast Ethernet interface, auto-QoS generates queue-set 1 (which is the default).
- For a Gigabit Ethernet interface, auto-QoS generates queue-set 2.

This is the enhanced configuration for the **auto qos voip cisco-phone** command:

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

This is the enhanced configuration for the **auto qos voip cisco-softphone** command:

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER

Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

**auto qos voip**

```

Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY

```

**Examples**

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the switch or router connected to the port is a trusted device:

```
Switch(config-if)# auto qos voip trust
```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug auto qos</b>	Enables debugging of the auto-QoS feature.
<b>mls qos cos</b>	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
<b>mls qos map</b>	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
<b>mls qos queue-set output buffers</b>	Allocates buffers to a queue-set.
<b>mls qos srr-queue input bandwidth</b>	Assigns shaped round robin (SRR) weights to an ingress queue.
<b>mls qos srr-queue input buffers</b>	Allocates the buffers between the ingress queues.
<b>mls qos srr-queue input cos-map</b>	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue input dscp-map</b>	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos srr-queue input priority-queue</b>	Configures the ingress priority queue and guarantees bandwidth.
<b>mls qos srr-queue output cos-map</b>	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue output dscp-map</b>	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos trust</b>	Configures the port trust state.
<b>queue-set</b>	Maps a port to a queue-set.
<b>show auto qos</b>	Displays auto-QoS information.
<b>show mls qos interface</b>	Displays QoS information at the port level.

Command	Description
<b>srr-queue bandwidth shape</b>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
<b>srr-queue bandwidth share</b>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

**boot buffersize**

# boot buffersize

Use the **boot buffersize** global configuration command on the switch stack or on a standalone switch to configure the NVRAM size. Use the **no** form of this command to return to the default.

**boot buffersize *size***

**no boot buffersize**

<b>Syntax Description</b>	<b>size</b> The NVRAM buffer size in KB. The valid range is from 4096 to 1048576.
---------------------------	---

**Defaults** The default NVRAM buffer size is 512 KB.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(55)SE	This command was introduced.

**Usage Guidelines** The default NVRAM buffer size is 512 KB. In some cases, the configuration file might be too large to save to NVRAM. Typically, this occurs when you have many switches in a switch stack. You can configure the size of the NVRAM buffer to support larger configuration files. The new NVRAM buffer size is synced to all current and new member switches.

After you configure the NVRAM buffer size, reload the switch or switch stack.

When you add a switch to a stack and the NVRAM size differs, the new switch syncs with the stack and reloads automatically.

**Examples** This example shows how to configure the NVRAM buffer size:

```
Switch(config)# boot buffersize 524288
Switch(config)# end
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show boot</b>	Displays the settings of the boot environment variables.

# boot config-file

Use the **boot config-file** global configuration command to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. Use the **no** form of this command to return to the default setting.

**boot config-file flash:/file-url**

**no boot config-file**

<b>Syntax Description</b>	<b>flash:/file-url</b> The path (directory) and name of the configuration file.				
<b>Defaults</b>	The default configuration file is flash:config.text.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>					
<b>Usage Guidelines</b>	Filenames and directory names are case sensitive. This command changes the setting of the CONFIG_FILE environment variable. For more information, see <a href="#">Appendix A, “Catalyst 3750 Switch Bootloader Commands.”</a>				
<b>Related Commands</b>	<table border="1"><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td><a href="#">show boot</a></td><td>Displays the settings of the boot environment variables.</td></tr></tbody></table>	Command	Description	<a href="#">show boot</a>	Displays the settings of the boot environment variables.
Command	Description				
<a href="#">show boot</a>	Displays the settings of the boot environment variables.				

**boot enable-break**

Use the **boot enable-break** global configuration command to enable interrupting the automatic boot process. Use the **no** form of this command to return to the default setting.

**boot enable-break**

**no boot enable-break**

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

**Defaults** Disabled. The automatic boot process cannot be interrupted by pressing the Break key on the console.

**Command Modes** Global configuration

**Command History**

**Usage Guidelines** When you enter this command, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.



**Note** Despite the setting of this command, you can interrupt the automatic boot process at any time by pressing the MODE button on the switch front panel.

This command changes the setting of the ENABLE\_BREAK environment variable. For more information, see [Appendix A, “Catalyst 3750 Switch Bootloader Commands.”](#)

**Related Commands**

Command	Description
<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# boot helper

Use the **boot helper** global configuration command to dynamically load files during boot loader initialization to extend or patch the functionality of the boot loader. Use the **no** form of this command to return to the default.

**boot helper** *filesystem:/file-url ...*

**no boot helper**

<b>Syntax Description</b>	<b>filesystem:</b> Alias for a flash file system. Use <b>flash:</b> for the system board flash device. <b>/file-url</b> The path (directory) and a list of loadable files to dynamically load during loader initialization. Separate each image name with a semicolon.
---------------------------	---

<b>Defaults</b>	No helper files are loaded.
-----------------	-----------------------------

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

## Command History

### Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the **HELPER** environment variable. For more information, see [Appendix A, “Catalyst 3750 Switch Bootloader Commands.”](#)

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show boot</b>	Displays the settings of the boot environment variables.

**boot helper-config-file**

Use the **boot helper-config-file** global configuration command to specify the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG\_FILE environment variable is used by all versions of Cisco IOS that are loaded. Use the **no** form of this command to return to the default setting.

**boot helper-config-file** *filesystem:/file-url*

**no boot helper-config file**

<b>Syntax Description</b>	<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
	<i>/file-url</i>	The path (directory) and helper configuration file to load.

**Defaults** No helper configuration file is specified.

**Command Modes** Global configuration

**Command History**

**Usage Guidelines** This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the **HELPER\_CONFIG\_FILE** environment variable. For more information, see [Appendix A, “Catalyst 3750 Switch Bootloader Commands.”](#)

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# boot manual

Use the **boot manual** global configuration command to enable manually booting the switch during the next boot cycle. Use the **no** form of this command to return to the default setting.

**boot manual**

**no boot manual**

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

**Defaults** Manual booting is disabled.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

The next time you reboot the system, the switch is in boot loader mode, which is shown by the *switch:* prompt. To boot up the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the MANUAL\_BOOT environment variable. For more information, see [Appendix A, “Catalyst 3750 Switch Bootloader Commands.”](#)

### Related Commands

Command	Description
<b>show boot</b>	Displays the settings of the boot environment variables.

**boot private-config-file**

# boot private-config-file

Use the **boot private-config-file** global configuration command to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration. Use the **no** form of this command to return to the default setting.

**boot private-config-file** *filename*

**no boot private-config-file**

<b>Syntax Description</b>	<i>filename</i>	The name of the private configuration file.
<b>Defaults</b>		The default configuration file is <i>private-config</i> .
<b>Command Modes</b>		Global configuration
<b>Command History</b>		
<b>Usage Guidelines</b>		Filenames are case sensitive.
<b>Examples</b>		This example shows how to specify the name of the private configuration file to be <i>pconfig</i> : Switch(config)# <b>boot private-config-file pconfig</b>
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show boot</a>	Displays the settings of the boot environment variables.

# boot system

Use the **boot system** global configuration command to specify the Cisco IOS image to load during the next boot cycle. Use the **no** form of this command to return to the default setting.

**boot system** *filesystem:/file-url ...*

**no boot system**

<b>Syntax Description</b>	<p><b>filesystem:</b> Alias for a flash file system. Use <b>flash:</b> for the system board flash device.</p> <p><b>/file-url</b> The path (directory) and name of a bootable image. Separate image names with a semicolon.</p>
---------------------------	---

<b>Defaults</b>	The switch attempts to automatically boot up the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.
-----------------	--

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

## Command History

### Usage Guidelines

Filenames and directory names are case sensitive.

If you are using the **archive download-sw** privileged EXEC command to maintain system images, you never need to use the **boot system** command. The **boot system** command is automatically manipulated to load the downloaded image.

This command changes the setting of the BOOT environment variable. For more information, see [Appendix A, “Catalyst 3750 Switch Bootloader Commands.”](#)

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>show boot</b></a>	Displays the settings of the boot environment variables.

**channel-group**

# channel-group

Use the **channel-group** interface configuration command to assign an Ethernet port to an EtherChannel group, to enable an EtherChannel mode, or both. Use the **no** form of this command to remove an Ethernet port from an EtherChannel group.

**channel-group** *channel-group-number* **mode** {**active** | {**auto** [**non-silent**]}} | {**desirable** [**non-silent**]}} | **on** | **passive**}

**no channel-group**

PAgP modes:

**channel-group** *channel-group-number* **mode** {{**auto** [**non-silent**]}} | {**desirable** [**non-silent**]}}

LACP modes:

**channel-group** *channel-group-number* **mode** {**active** | **passive**}

On mode:

**channel-group** *channel-group-number* **mode** **on**

**Syntax Description**

<i>channel-group-number</i>	Specify the channel group number. The range is 1 to .
<b>mode</b>	Specify the EtherChannel mode.
<b>active</b>	Unconditionally enable Link Aggregation Control Protocol (LACP).  Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.
<b>auto</b>	Enable the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.  Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When <b>auto</b> is enabled, silent operation is the default.
<b>desirable</b>	Unconditionally enable PAgP.  Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. An EtherChannel is formed with another port group that is in the desirable or auto mode. When <b>desirable</b> is enabled, silent operation is the default.
<b>non-silent</b>	(Optional) Use in PAgP mode with the <b>auto</b> or <b>desirable</b> keyword when traffic is expected from the other device.
<b>on</b>	Enable <b>on</b> mode.  In <b>on</b> mode, a usable EtherChannel exists only when both connected port groups are in the <b>on</b> mode.
<b>passive</b>	Enable LACP only if a LACP device is detected.  Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

**Defaults** No channel groups are assigned.  
No mode is configured.

**Command Modes** Interface configuration

### Command History

**Usage Guidelines** For Layer 2 EtherChannels, you do not have to create a port-channel interface first by using the **interface port-channel** global configuration command before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port if the logical interface is not already created. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode.



### Caution

You should use care when using the **on** mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

**channel-group****Examples**

This example shows how to configure an EtherChannel on a single switch. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single switch. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>channel-protocol</b></a>	Restricts the protocol used on a port to manage channeling.
<a href="#"><b>interface port-channel</b></a>	Accesses or creates the port channel.
<a href="#"><b>show etherchannel</b></a>	Displays EtherChannel information for a channel.
<a href="#"><b>show lacp</b></a>	Displays LACP channel-group information.
<a href="#"><b>show pagp</b></a>	Displays PAgP channel-group information.
<a href="#"><b>show running-config</b></a>	Displays the current operating configuration.

# channel-protocol

Use the **channel-protocol** interface configuration command to restrict the protocol used on a port to manage channeling. Use the **no** form of this command to return to the default setting.

**channel-protocol {lacp | pagp}**

**no channel-protocol**

<b>Syntax Description</b>	<b>lacp</b> Configure an EtherChannel with the Link Aggregation Control Protocol (LACP). <b>pagp</b> Configure an EtherChannel with the Port Aggregation Protocol (PAgP).
---------------------------	--

**Defaults**      No protocol is assigned to the EtherChannel.

**Command Modes**      Interface configuration

## Command History

**Usage Guidelines**      Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

**Examples**      This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Switch(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel [channel-group-number] protocol** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>channel-group</b>	Assigns an Ethernet port to an EtherChannel group.
	<b>show etherchannel protocol</b>	Displays protocol information the EtherChannel.

**cisp enable**

# cisp enable

Use the **cisp enable** global configuration command to enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.

**cisp enable**

**no cisp enable**

<b>Syntax Description</b>	<b>cisp enable</b>	Enable CISP.
<b>Defaults</b>	There is no default setting.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.
<b>Usage Guidelines</b>	<p>The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, the VTP domain name must be the same, and the VTP mode must be <i>server</i>.</p> <p>When you configure VTP mode, to avoid the MD5 checksum mismatch error, verify that:</p> <ul style="list-style-type: none"> <li>• VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.</li> <li>• Both switches have the different configuration revision numbers.</li> </ul>	
<b>Examples</b>	<p>This example shows how to enable CISP:</p> <pre>switch(config)# <b>cisp enable</b></pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x credentials (global configuration) profile</a>	Configures a profile on a supplicant switch.
	<a href="#">show cisp</a>	Displays CISP information for a specified interface.

# class

Use the **class** policy-map configuration command to define a traffic classification match criteria (through the **police**, **set**, and **trust** policy-map class configuration commands) for the specified class-map name. Use the **no** form of this command to delete an existing class map.

```
class {class-map-name | class-default}
no class {class-map-name | class-default}
```

<b>Syntax Description</b>	<b>class-map-name</b> Specifies the name of the class map. <b>class-default</b> System default class that matches unclassified packets.
---------------------------	--

**Defaults**      No class-maps are defined.

**Command Modes**      Policy-map configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(55)SE	The <b>class-default</b> keyword was added.

**Usage Guidelines**      Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter policy-map class configuration mode, and these configuration commands are available:

- **exit**—Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**—Returns a command to its default setting.
- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** and **police aggregate** policy-map class commands.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see the **set** command.
- **trust**—Defines a trust state for traffic classified with the **class** or the **class-map** command. For more information, see the **trust** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map global configuration command**. When you need a new classification that is not shared with any other ports, use the **class** command. When the map is shared among many ports, use the **class-map** command.

**class**

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is considered to be default traffic.

**Examples**

This example shows how to create a policy map called *policy1*. When attached to the ingress direction, it matches all the incoming traffic defined in *class1*, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value received from the policed-DSCP map and then sent.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map:

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c) set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

This example shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Switch# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    trust cos
  Class class-default
    set dscp 10
Switch#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>class-map</b>	Creates a class map to be used for matching packets to the class whose name you specify.
<b>police</b>	Defines a policer for classified traffic.

Command	Description
<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<b>set</b>	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
<b>show policy-map</b>	Displays quality of service (QoS) policy maps.
<b>trust</b>	Defines a trust state for the traffic classified through the <b>class</b> policy-map configuration command or the <b>class-map</b> global configuration command.

# class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to the class name you specify and to enter class-map configuration mode. Use the **no** form of this command to delete an existing class map and to return to global configuration mode.

```
class-map [match-all | match-any] class-map-name
no class-map [match-all | match-any] class-map-name
```

Syntax Description	<b>match-all</b> (Optional) Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched.
	<b>match-any</b> (Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
	<i>class-map-name</i> Name of the class map.

<b>Defaults</b>	No class maps are defined.
	If neither the <b>match-all</b> or <b>match-any</b> keyword is specified, the default is <b>match-all</b> .

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

<b>Command History</b>	
<b>Usage Guidelines</b>	Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class-map.
- **exit**: exits from QoS class-map configuration mode.
- **match**: configures classification criteria. For more information, see the **match (class-map configuration)** command.
- **no**: removes a match statement from a class map.
- **rename**: renames the current class map. If you rename a class map with a name that is already used, the message **A class-map with this name already exists** appears.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

Only one access control list (ACL) can be configured in a class map. The ACL can have multiple access control entries (ACEs).

**Examples**

This example shows how to configure the class map called *class1* with one match criterion, which is an access list called *103*:

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to delete the class map *class1*:

```
Switch(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">class</a>	Defines a traffic classification match criteria (through the <b>police</b> , <b>set</b> , and <b>trust</b> policy-map class configuration commands) for the specified class-map name.
<a href="#">match (class-map configuration)</a>	Defines the match criteria to classify traffic.
<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#">show class-map</a>	Displays QoS class maps.

---

■ **clear arp inspection log**

# clear arp inspection log

Use the **clear ip arp inspection log** privileged EXEC command to clear the dynamic Address Resolution Protocol (ARP) inspection log buffer.

**clear ip arp inspection log**

---

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

---

**Defaults** No default is defined.

---

**Command Modes** Privileged EXEC

---

**Command History**

**Examples** This example shows how to clear the contents of the log buffer:

```
Switch# clear ip arp inspection log
```

You can verify that the log was cleared by entering the **show ip arp inspection log** privileged command.

---

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.
<a href="#">ip arp inspection vlan logging</a>	Controls the type of packets that are logged per VLAN.
<a href="#">show inventory log</a>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

# clear dot1x

Use the **clear dot1x** privileged EXEC command to clear IEEE 802.1x information for the switch or for the specified port.

**clear dot1x {all | interface *interface-id*}**

<b>Syntax Description</b>	<b>all</b> Clear all IEEE 802.1x information for the switch. <b>interface <i>interface-id</i></b> Clear IEEE 802.1x information for the specified interface.
---------------------------	---

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

<b>Usage Guidelines</b>	You can clear all the information by using the <b>clear dot1x all</b> command, or you can clear only the information for the specified interface by using the <b>clear dot1x interface <i>interface-id</i></b> command.
-------------------------	---

<b>Examples</b>	This example shows how to clear all IEEE 802.1x information:
-----------------	--

```
Switch# clear dot1x all
```

This example shows how to clear IEEE 802.1x information for the specified interface:

```
Switch# clear dot1x interface gigabitethernet1/1
```

You can verify that the information was deleted by entering the **show dot1x** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show dot1x</a>	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

**■ clear eap sessions**

# clear eap sessions

Use the **clear eap sessions** privileged EXEC command to clear Extensible Authentication Protocol (EAP) session information for the switch or for the specified port.

```
clear eap sessions [credentials name [interface interface-id] | interface interface-id | method name | transport name] [credentials name | interface interface-id | transport name] ...
```

<b>Syntax Description</b>	<b>credentials name</b> Clear EAP credential information for the specified profile. <b>interface interface-id</b> Clear EAP information for the specified interface. <b>method name</b> Clear EAP information for the specified method. <b>transport name</b> Clear EAP transport information for the specified lower level.
---------------------------	---

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

**Usage Guidelines** You can clear all counters by using the **clear eap sessions** command, or you can clear only the specific information by using the keywords.

**Examples** This example shows how to clear all EAP information:

```
Switch# clear eap
```

This example shows how to clear EAP-session credential information for the specified profile:

```
Switch# clear eap sessions credential type1
```

You can verify that the information was deleted by entering the **show dot1x** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show eap</b>	Displays EAP registration and session information for the switch or for the specified port

# clear errdisable interface

Use the **clear errdisable interface** privileged EXEC command to re-enable a VLAN that was error disabled.

**clear errdisable interface *interface-id* vlan [vlan-list]**

<b>Syntax Description</b>	<i>vlan list</i> (Optional) Specify a list of VLANs to be re-enabled. If a <i>vlan-list</i> is not specified, then all VLANs are re-enabled.
---------------------------	---

<b>Command Default</b>	No default is defined
------------------------	-----------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(37)SE	This command was introduced.

<b>Usage Guidelines</b>	You can re-enable a port by using the <b>shutdown</b> and <b>no shutdown</b> interface configuration commands, or you can clear error disable for VLANs by using the <b>clear errdisable interface</b> command.
-------------------------	---

<b>Examples</b>	This example shows how to re-enable all VLANs that were error-disabled on port 2.
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>errdisable detect cause</b></a>	Enables error-disabled detection for a specific cause or all causes.
	<a href="#"><b>errdisable recovery</b></a>	Configures the recovery mechanism variables.
	<a href="#"><b>show errdisable detect</b></a>	Displays error-disabled detection status.
	<a href="#"><b>show errdisable recovery</b></a>	Display error-disabled recovery timer information.
	<a href="#"><b>show interfaces status err-disabled</b></a>	Displays interface status of a list of interfaces in error-disabled state.

**■ clear ip arp inspection statistics**

# clear ip arp inspection statistics

Use the **clear ip arp inspection statistics** privileged EXEC command to clear the dynamic Address Resolution Protocol (ARP) inspection statistics.

**clear ip arp inspection statistics [vlan *vlan-range*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-range</i></b> (Optional) Clear statistics for the specified VLAN or VLANs. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.				
<b>Defaults</b>	No default is defined.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>					
<b>Examples</b>	This example shows how to clear the statistics for VLAN 1: <pre>Switch# clear ip arp inspection statistics vlan 1</pre> You can verify that the statistics were deleted by entering the <b>show ip arp inspection statistics vlan 1</b> privileged EXEC command.				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th> <th><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><a href="#">show inventory statistics</a></td> <td>Displays statistics for forwarded, dropped, MAC validation failure, and IP validation failure packets for all VLANs or the specified VLAN.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">show inventory statistics</a>	Displays statistics for forwarded, dropped, MAC validation failure, and IP validation failure packets for all VLANs or the specified VLAN.
<b>Command</b>	<b>Description</b>				
<a href="#">show inventory statistics</a>	Displays statistics for forwarded, dropped, MAC validation failure, and IP validation failure packets for all VLANs or the specified VLAN.				

# clear ip dhcp snooping

Use the **clear ip dhcp snooping** privileged EXEC command to clear the DHCP snooping binding database, the DHCP snooping binding database agent statistics, or the DHCP snooping statistics counters.

```
clear ip dhcp snooping {binding {* | ip-address | interface interface-id | vlan vlan-id} | database statistics | statistics}
```

## Syntax Description

<b>binding</b>	Clear the DHCP snooping binding database.
<b>*</b>	Clear all automatic bindings.
<b>ip-address</b>	Clear the binding entry IP address.
<b>interface interface-id</b>	Clear the binding input interface.
<b>vlan vlan-id</b>	Clear the binding entry VLAN.
<b>database statistics</b>	Clear the DHCP snooping binding database agent statistics.
<b>statistics</b>	Clear the DHCP snooping statistics counter.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(37)SE	The <b>statistics</b> keyword was introduced.
12.2(44)SE	The <b>*, ip-address, interface interface-id, and vlan vlan-id</b> keywords were introduced.

## Usage Guidelines

When you enter the **clear ip dhcp snooping database statistics** command, the switch does not update the entries in the binding database and in the binding file before clearing the statistics.

## Examples

This example shows how to clear the DHCP snooping binding database agent statistics:

```
Switch# clear ip dhcp snooping database statistics
```

You can verify that the statistics were cleared by entering the **show ip dhcp snooping database** privileged EXEC command.

This example shows how to clear the DHCP snooping statistics counters:

```
Switch# clear ip dhcp snooping statistics
```

You can verify that the statistics were cleared by entering the **show ip dhcp snooping statistics** user EXEC command.

■ **clear ip dhcp snooping**

Related Commands	Command	Description
	<b>ip dhcp snooping</b>	Enables DHCP snooping on a VLAN.
	<b>ip dhcp snooping database</b>	Configures the DHCP snooping binding database agent or the binding file.
	<b>show ip dhcp snooping binding</b>	Displays the status of DHCP snooping database agent.
	<b>show ip dhcp snooping database</b>	Displays the DHCP snooping binding database agent statistics.
	<b>show ip dhcp snooping statistics</b>	Displays the DHCP snooping statistics.

# clear lacp

Use the **clear lacp** privileged EXEC command to clear Link Aggregation Control Protocol (LACP) channel-group counters.

**clear lacp {channel-group-number counters | counters}**

<b>Syntax Description</b>	<p><i>channel-group-number</i> (Optional) Channel group number. The range is 1 to .</p> <p><b>counters</b> Clear traffic counters.</p>
---------------------------	--

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

<b>Usage Guidelines</b>	You can clear all counters by using the <b>clear lacp counters</b> command, or you can clear only the counters for the specified channel group by using the <b>clear lacp channel-group-number counters</b> command.
-------------------------	--

<b>Examples</b>	This example shows how to clear all channel-group information:
-----------------	--

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:
--

```
Switch# clear lacp 4 counters
```

You can verify that the information was deleted by entering the <b>show lacp counters</b> or the <b>show lacp 4 counters</b> privileged EXEC command.
---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show lacp</a>	Displays LACP channel-group information.

---

■ **clear mac address-table**

## clear mac address-table

Use the **clear mac address-table** privileged EXEC command to delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. This command also clears the MAC address notification global counters.

```
clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id] | notification}
```

Syntax Description	
<b>dynamic</b>	Delete all dynamic MAC addresses.
<b>dynamic address</b> <i>mac-addr</i>	(Optional) Delete the specified dynamic MAC address.
<b>dynamic interface</b> <i>interface-id</i>	(Optional) Delete all dynamic MAC addresses on the specified physical port or port channel.
<b>dynamic vlan</b> <i>vlan-id</i>	(Optional) Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
<b>notification</b>	Clear the notifications in the history table and reset the counters.

---

**Defaults** No default is defined.

---

**Command Modes** Privileged EXEC

---

### Command History

#### Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

Related Commands	Command	Description
	<b>mac address-table notification</b>	Enables the MAC address notification feature.
	<b>show mac access-group</b>	Displays the MAC address table static and dynamic entries.
	<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>snmp trap mac-notification change</b>	Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific interface.

---

■ **clear mac address-table move update**

# clear mac address-table move update

Use the **clear mac address-table move update** privileged EXEC command to clear the mac address-table-move update-related counters.

## **clear mac address-table move update**

---

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

---

**Defaults** No default is defined.

---

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(25)SED	This command was introduced.

---

**Examples** This example shows how to clear the mac address-table move update related counters.

```
Switch# clear mac address-table move update
```

You can verify that the information was cleared by entering the **show mac address-table move update** privileged EXEC command.

Related Commands	Command	Description
	<b>mac address-table move update {receive   transmit}</b>	Configures MAC address-table move update on the switch.
	<b>show mac address-table move update</b>	Displays the MAC address-table move update information on the switch.

# clear nmsp statistics

Use the **clear nmsp statistics** privileged EXEC command to clear the Network Mobility Services Protocol (NMSP) statistics. This command is available only when your switch is running the cryptographic (encrypted) software image.

## clear nmsp statistics

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

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Examples** This example shows how to clear NMSP statistics:

```
Switch# clear nmsp statistics
```

You can verify that information was deleted by entering the **show nmsp statistics** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show nmsp</a>	Displays the NMSP information.

**■ clear pagp**

# clear pagp

Use the **clear pagp** privileged EXEC command to clear Port Aggregation Protocol (PAgP) channel-group information.

**clear pagp {channel-group-number counters | counters}**

<b>Syntax Description</b>	<i>channel-group-number</i> (Optional) Channel group number. The range is 1 to .
	<b>counters</b> Clear traffic counters.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp channel-group-number counters** command.

**Examples** This example shows how to clear all channel-group information:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

You can verify that information was deleted by entering the **show pagp** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show pagp</a>	Displays PAgP channel-group information.

# clear port-security

Use the **clear port-security** privileged EXEC command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

```
clear port-security {all | configured | dynamic | sticky} [[address mac-addr | interface
interface-id] [vlan {vlan-id | {access | voice}}]]]
```

Syntax Description	<b>all</b> Delete all secure MAC addresses. <b>configured</b> Delete configured secure MAC addresses. <b>dynamic</b> Delete secure MAC addresses auto-learned by hardware. <b>sticky</b> Delete secure MAC addresses, either auto-learned or configured. <b>address mac-addr</b> (Optional) Delete the specified dynamic secure MAC address. <b>interface interface-id</b> (Optional) Delete all the dynamic secure MAC addresses on the specified physical port or VLAN. <b>vlan</b> (Optional) Delete the specified secure MAC address from the specified VLAN. Enter one of these options after you enter the <b>vlan</b> keyword: <ul style="list-style-type: none"> <li>• <i>vlan-id</i>—On a trunk port, specify the VLAN ID of the VLAN on which this address should be cleared.</li> <li>• <b>access</b>—On an access port, clear the specified secure MAC address on the access VLAN.</li> <li>• <b>voice</b>—On an access port, clear the specified secure MAC address on the voice VLAN.</li> </ul> <b>Note</b> The <b>voice</b> keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
<b>Defaults</b>	No default is defined.
<b>Command Modes</b>	Privileged EXEC
<b>Command History</b>	
<b>Examples</b>	<p>This example shows how to clear all secure addresses from the MAC address table:</p> <pre>Switch# <b>clear port-security all</b></pre> <p>This example shows how to remove a specific configured secure address from the MAC address table:</p> <pre>Switch# <b>clear port-security configured address 0008.0070.0007</b></pre> <p>This example shows how to remove all the dynamic secure addresses learned on a specific interface:</p> <pre>Switch# <b>clear port-security dynamic interface gigabitethernet0/1</b></pre>

**■ clear port-security**

This example shows how to remove all the dynamic secure addresses from the address table:

```
Switch# clear port-security dynamic
```

You can verify that the information was deleted by entering the **show port-security** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>switchport port-security</b></a>	Enables port security on an interface.
<a href="#"><b>switchport port-security mac-address</b> <i>mac-address</i></a>	Configures secure MAC addresses.
<a href="#"><b>switchport port-security maximum</b> <i>value</i></a>	Configures a maximum number of secure MAC addresses on a secure interface.
<a href="#"><b>show port-security</b></a>	Displays the port security settings defined for an interface or for the switch.

# clear psp counter

To clear the protocol storm protection counter of packets dropped for all protocols, use the **clear psp counter** privileged EXEC command.

**clear psp counter [arp | igmp | dhcp]**

<b>Syntax Description</b>	<b>arp</b> (Optional) Clear the counter of dropped packets for ARP and ARP snooping. <b>dhcp</b> (Optional) Clear the counter of dropped packets for DHCP and DHCP snooping. <b>igmp</b> (Optional) Clear the counter of dropped packets for IGMP and IGMP snooping.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(58)SE	This command was introduced.

<b>Examples</b>	In this example, the protocol storm protection counter for DHCP is cleared.
-----------------	---

```
Switch# clear psp counter dhcp
Switch#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>psp {arp   dhcp   igmp} pps value</b>	Configures protocol storm protection for ARP, DHCP, or IGMP.
	<b>show psp config</b>	Displays the protocol storm protection configuration
	<b>show psp statistics</b>	Displays the number of dropped packets.

---

■ **clear spanning-tree counters**

# clear spanning-tree counters

Use the **clear spanning-tree counters** privileged EXEC command to clear the spanning-tree counters.

**clear spanning-tree counters [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to .
---------------------------	---

---

**Defaults** No default is defined.

---

**Command Modes** Privileged EXEC

---

**Command History**

**Usage Guidelines** If the *interface-id* is not specified, spanning-tree counters are cleared for all interfaces.

---

**Examples** This example shows how to clear spanning-tree counters for all interfaces:

```
Switch# clear spanning-tree counters
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree</a>	Displays spanning-tree state information.

# clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.

**clear spanning-tree detected-protocols [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to .
---------------------------	---

<b>Defaults</b>	No default is defined.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

<b>Usage Guidelines</b>	A switch running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2). However, the switch does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the <b>clear spanning-tree detected-protocols</b> command in this situation.
-------------------------	---

## Examples

This example shows how to restart the protocol migration process on a port:

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet0/1
```

## Related Commands

<b>Command</b>	<b>Description</b>
<a href="#">show spanning-tree</a>	Displays spanning-tree state information.
<a href="#">spanning-tree link-type</a>	Overrides the default link-type setting and enables rapid spanning-tree changes to the forwarding state.

**■ clear vmpls statistics**

# clear vmpls statistics

Use the **clear vmpls statistics** privileged EXEC command to clear the statistics maintained by the VLAN Query Protocol (VQP) client.

**clear vmpls statistics**

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

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

## Command History

**Examples** This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Switch# clear vmpls statistics
```

You can verify that information was deleted by entering the **show vmpls statistics** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">show vmpls</a>	Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers.

# clear vtp counters

Use the **clear vtp counters** privileged EXEC command to clear the VLAN Trunking Protocol (VTP) and pruning counters.

## clear vtp counters

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

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

## Command History

**Examples** This example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">show vtp</a>	Displays general information about the VTP management domain, status, and counters.

**cluster commander-address**

## cluster commander-address

You do not need to enter this command from a standalone cluster member switch. The cluster command switch automatically provides its MAC address to cluster member switches when these switches join the cluster. The cluster member switch adds this information and other cluster information to its running configuration file. Use the **no** form of this global configuration command from the cluster member switch console port to remove the switch from a cluster only during debugging or recovery procedures.

**cluster commander-address *mac-address* [member *number* name *name*]**

**no cluster commander-address**

---

### Syntax Description

<b><i>mac-address</i></b>	MAC address of the cluster command switch.
<b><i>member number</i></b>	(Optional) Number of a configured cluster member switch. The range is 0 to 15.
<b><i>name name</i></b>	(Optional) Name of the configured cluster up to 31 characters.

---



---

### Defaults

The switch is not a member of any cluster.

---

### Command Modes

Global configuration

---

### Command History

---

### Usage Guidelines

This command is available only on the cluster command switch.

A cluster member can have only one cluster command switch.

The cluster member switch retains the identity of the cluster command switch during a system reload by using the *mac-address* parameter.

You can enter the **no** form on a cluster member switch to remove it from the cluster during debugging or recovery procedures. You would normally use this command from the cluster member switch console port only when the member has lost communication with the cluster command switch. With normal switch configuration, we recommend that you remove cluster member switches only by entering the **no cluster member *n*** global configuration command on the cluster command switch.

When a standby cluster command switch becomes active (becomes the cluster command switch), it removes the cluster commander address line from its configuration.

**Examples**

This is partial sample output from the running configuration of a cluster member.

```
Switch(config)# show running-configuration  
<output truncated>  
cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster  
<output truncated>
```

This example shows how to remove a member from the cluster by using the cluster member console.

```
Switch # configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)# no cluster commander-address
```

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

**Related Commands**

Command	Description
<a href="#">debug cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.

---

 ■ cluster discovery hop-count

# cluster discovery hop-count

Use the **cluster discovery hop-count** global configuration command on the cluster command switch to set the hop-count limit for extended discovery of candidate switches. Use the **no** form of this command to return to the default setting.

**cluster discovery hop-count *number***

**no cluster discovery hop-count**

---

<b>Syntax Description</b>	<i>number</i>	Number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7.
---------------------------	---------------	---

---

<b>Defaults</b>	The hop count is set to 3.
-----------------	----------------------------

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

## Command History

<b>Usage Guidelines</b>	This command is available only on the cluster command switch. This command does not operate on cluster member switches.  If the hop count is set to 1, it disables extended discovery. The cluster command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered cluster member switch and the first discovered candidate switch.
-------------------------	--

<b>Examples</b>	This example shows how to set hop count limit to 4. This command is executed on the cluster command switch.
-----------------	---

```
Switch(config)# cluster discovery hop-count 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.
	<a href="#">show cluster candidates</a>	Displays a list of candidate switches.

---

# cluster enable

Use the **cluster enable** global configuration command on a command-capable switch to enable it as the cluster command switch, assign a cluster name, and to optionally assign a member number to it. Use the **no** form of the command to remove all members and to make the cluster command switch a candidate switch.

**cluster enable** *name* [*command-switch-member-number*]

**no cluster enable**

Syntax Description	<i>name</i> Name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores. <i>command-switch-member-number</i> (Optional) Assign a member number to the cluster command switch of the cluster. The range is 0 to 15.
--------------------	---

## Defaults

The switch is not a cluster command switch.

No cluster name is defined.

The member number is 0 when the switch is the cluster command switch.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

Enter this command on any command-capable switch that is not part of any cluster. This command fails if a device is already configured as a member of the cluster.

You must name the cluster when you enable the cluster command switch. If the switch is already configured as the cluster command switch, this command changes the cluster name if it is different from the previous cluster name.

## Examples

This example shows how to enable the cluster command switch, name the cluster, and set the cluster command switch member number to 4.

```
Switch(config)# cluster enable Engineering-IDF4 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command on the cluster command switch.

## Related Commands

Command	Description
<a href="#">show cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.

**cluster holdtime**

# cluster holdtime

Use the **cluster holdtime** global configuration command on the cluster command switch to set the duration in seconds before a switch (either the command or cluster member switch) declares the other switch down after not receiving heartbeat messages. Use the **no** form of this command to set the duration to the default value.

**cluster holdtime** *holdtime-in-secs*

**no cluster holdtime**

---

<b>Syntax Description</b>	<i>holdtime-in-secs</i>	Duration in seconds before a switch (either a command or cluster member switch) declares the other switch down. The range is 1 to 300 seconds.
---------------------------	-------------------------	--

---

**Defaults** The default holdtime is 80 seconds.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** Enter this command with the **cluster timer** global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

**Examples** This example shows how to change the interval timer and the duration on the cluster command switch.

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

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

---

## Related Commands

Command	Description
<b>show cluster</b>	Displays the cluster status and a summary of the cluster to which the switch belongs.

---

# cluster member

Use the **cluster member** global configuration command on the cluster command switch to add candidates to a cluster. Use the **no** form of the command to remove members from the cluster.

**cluster member [n] mac-address H.H.H [password enable-password] [vlan vlan-id]**

**no cluster member n**

Syntax Description	<p><b>n</b> The number that identifies a cluster member. The range is 0 to 15.</p> <p><b>mac-address H.H.H</b> MAC address of the cluster member switch in hexadecimal format.</p> <p><b>password enable-password</b> Enable password of the candidate switch. The password is not required if there is no password on the candidate switch.</p> <p><b>vlan vlan-id</b> (Optional) VLAN ID through which the candidate is added to the cluster by the cluster command switch. The range is 1 to 4094.</p>
--------------------	---

**Defaults** A newly enabled cluster command switch has no associated cluster members.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

Enter this command only on the cluster command switch to add a candidate to or remove a member from the cluster. If you enter this command on a switch other than the cluster command switch, the switch rejects the command and displays an error message.

You must enter a member number to remove a switch from the cluster. However, you do not need to enter a member number to add a switch to the cluster. The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

You must enter the enable password of the candidate switch for authentication when it joins the cluster. The password is not saved in the running or startup configuration. After a candidate switch becomes a member of the cluster, its password becomes the same as the cluster command-switch password.

If a switch does not have a configured hostname, the cluster command switch appends a member number to the cluster command-switch hostname and assigns it to the cluster member switch.

If you do not specify a VLAN ID, the cluster command switch automatically chooses a VLAN and adds the candidate to the cluster.

### Examples

This example shows how to add a switch as member 2 with MAC address 00E0.1E00.2222 and the password *key* to a cluster. The cluster command switch adds the candidate to the cluster through VLAN 3.

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

**cluster member**

This example shows how to add a switch with MAC address 00E0.1E00.3333 to the cluster. This switch does not have a password. The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

You can verify your settings by entering the **show cluster members** privileged EXEC command on the cluster command switch.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>show cluster</b></a>	Displays the cluster status and a summary of the cluster to which the switch belongs.
	<a href="#"><b>show cluster candidates</b></a>	Displays a list of candidate switches.
	<a href="#"><b>show cluster members</b></a>	Displays information about the cluster members.

# cluster outside-interface

Use the **cluster outside-interface** global configuration command on the cluster command switch to configure the outside interface for cluster Network Address Translation (NAT) so that a member without an IP address can communicate with devices outside the cluster. Use the **no** form of this command to return to the default setting.

**cluster outside-interface *interface-id***

**no cluster outside-interface**

---

<b>Syntax Description</b>	<i>interface-id</i>	Interface to serve as the outside interface. Valid interfaces include physical interfaces, port-channels, or VLANs. The port-channel range is 1 to . The VLAN range is 1 to 4094.
---------------------------	---------------------	---

---

**Defaults** The default outside interface is automatically selected by the cluster command switch.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** Enter this command only on the cluster command switch. If you enter this command on a cluster member switch, an error message appears.

**Examples** This example shows how to set the outside interface to VLAN 1:

```
Switch(config)# cluster outside-interface vlan 1
```

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

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show running-config</b>	Displays the current operating configuration.

---

**cluster run**

## cluster run

Use the **cluster run** global configuration command to enable clustering on a switch. Use the **no** form of this command to disable clustering on a switch.

**cluster run**

**no cluster run**

---

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

---

**Defaults** Clustering is enabled on all switches.

---

**Command Modes** Global configuration

---

**Command History**

**Usage Guidelines** When you enter the **no cluster run** command on a cluster command switch, the cluster command switch is disabled. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a cluster member switch, it is removed from the cluster. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a switch that is not part of a cluster, clustering is disabled on this switch. This switch cannot then become a candidate switch.

---

**Examples** This example shows how to disable clustering on the cluster command switch:

```
Switch(config)# no cluster run
```

You can verify your setting by entering the **show cluster** privileged EXEC command.

---

**Related Commands**

Command	Description
<a href="#">show cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.

# cluster standby-group

Use the **cluster standby-group** global configuration command to enable cluster command-switch redundancy by binding the cluster to an existing Hot Standby Router Protocol (HSRP). Entering the routing-redundancy keyword enables the same HSRP group to be used for cluster command-switch redundancy and routing redundancy. Use the **no** form of this command to return to the default setting.

```
cluster standby-group HSRP-group-name [routing-redundancy]
no cluster standby-group
```

<b>Syntax Description</b>	<i>HSRP-group-name</i> Name of the HSRP group that is bound to the cluster. The group name is limited to 32 characters. <b>routing-redundancy</b> (Optional) Enable the same HSRP standby group to be used for cluster command-switch redundancy and routing redundancy.
---------------------------	---

**Defaults**      The cluster is not bound to any HSRP group.

**Command Modes**      Global configuration

## Command History

### Usage Guidelines

Enter this command only on the cluster command switch. If you enter it on a cluster member switch, an error message appears.

The cluster command switch propagates the cluster-HSRP binding information to all cluster-HSRP capable members. Each cluster member switch stores the binding information in its NVRAM. The HSRP group name must be a valid standby group; otherwise, the command exits with an error.

The same group name should be used on all members of the HSRP standby group that is to be bound to the cluster. The same HSRP group name should also be used on all cluster-HSRP capable members for the HSRP group that is to be bound. (When not binding a cluster to an HSRP group, you can use different names on the cluster commander and the members.)

### Examples

This example shows how to bind the HSRP group named *my\_hsrp* to the cluster. This command is executed on the cluster command switch.

```
Switch(config)# cluster standby-group my_hsrp
```

This example shows how to use the same HSRP group named *my\_hsrp* for routing redundancy and cluster redundancy.

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
```

This example shows the error message when this command is executed on a cluster command switch and the specified HSRP standby group does not exist:

```
Switch(config)# cluster standby-group my_hsrp
%ERROR: Standby (my_hsrp) group does not exist
```

**cluster standby-group**

This example shows the error message when this command is executed on a cluster member switch:

```
Switch(config)# cluster standby-group my_hsrp routing-redundancy
%ERROR: This command runs on a cluster command switch
```

You can verify your settings by entering the **show cluster** privileged EXEC command. The output shows whether redundancy is enabled in the cluster.

Related Commands	Command	Description
	<b>standby ip</b>	Enables HSRP on the interface.
	<b>show cluster</b>	Displays the cluster status and a summary of the cluster to which the switch belongs.
	<b>show standby</b>	Displays standby group information.

# cluster timer

Use the **cluster timer** global configuration command on the cluster command switch to set the interval in seconds between heartbeat messages. Use the **no** form of this command to set the interval to the default value.

**cluster timer** *interval-in-secs*

**no cluster timer**

<b>Syntax Description</b>	<i>interval-in-secs</i>	Interval in seconds between heartbeat messages. The range is 1 to 300 seconds.
---------------------------	-------------------------	--

<b>Defaults</b>	The interval is 8 seconds.
-----------------	----------------------------

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

## Command History

**Usage Guidelines** Enter this command with the **cluster holdtime** global configuration command only on the cluster command switch. The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the heartbeat interval timer (**cluster timer**). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of heartbeat messages to be missed in a row to declare a switch down.

**Examples** This example shows how to change the heartbeat interval timer and the duration on the cluster command switch:

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cluster</a>	Displays the cluster status and a summary of the cluster to which the switch belongs.

---

■ **define interface-range**

# define interface-range

Use the **define interface-range** global configuration command to create an interface-range macro. Use the **no** form of this command to delete the defined macro.

**define interface-range** *macro-name interface-range*

**no define interface-range** *macro-name interface-range*

<b>Syntax Description</b>	<i>macro-name</i> Name of the interface-range macro; up to 32 characters. <i>interface-range</i> Interface range; for valid values for interface ranges, see “Usage Guidelines.”
---------------------------	---

---

**Defaults** This command has no default setting.

---

**Command Modes** Global configuration

---

## Command History

**Usage Guidelines** The macro name is a 32-character maximum character string.

A macro can contain up to five ranges.

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.

When entering the *interface-range*, use this format:

- *type {first-interface} - {last-interface}*
- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 - 2** is a valid range; **gigabitethernet 0/1-2** is not a valid range.

Valid values for *type* and *interface*:

- **vlan** *vlan-id*, where the VLAN ID is 1 to 4094  
VLAN interfaces must have been configured with the **interface vlan** command (the **show running-config** privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-config** command cannot be used in *interface-ranges*.
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to
- **fastethernet** *module/{first port} - {last port}*
- **gigabitethernet** *module/{first port} - {last port}*

For physical interfaces:

- module is always 0.
- the range is *type 0/number - number* (for example, **gigabitethernet 0/1 - 2**).

When you define a range, you must enter a space before the hyphen (-), for example:

- **gigabitethernet0/1 - 2**

You can also enter multiple ranges. When you define multiple ranges, you must enter a space after the first entry before the comma (,). The space after the comma is optional, for example:

- **fastethernet0/3, gigabitetherent0/1 - 2**
- **fastethernet0/3 -4, gigabitetherent0/1 - 2**

---

**Examples**

This example shows how to create a multiple-interface macro:

---

**Related Commands**

Command	Description
<a href="#">interface range</a>	Executes a command on multiple ports at the same time.
<a href="#">show running-config</a>	Displays the current operating configuration, including defined macros.

---

**■ delete**

# delete

Use the **delete** privileged EXEC command to delete a file or directory on the flash memory device.

**delete [/force] [/recursive] filesystem:/file-url**

---

## Syntax Description

<b>/force</b>	(Optional) Suppress the prompt that confirms the deletion.
<b>/recursive</b>	(Optional) Delete the named directory and all subdirectories and the files contained in it.
<b>filesystem:</b>	Alias for a flash file system.
<b>Note</b>	The syntax for the local flash file system: <b>flash:</b>
<b>/file-url</b>	The path (directory) and filename to delete.

---



---

## Command Modes

Privileged EXEC

---

## Command History

### Usage Guidelines

If you use the **/force** keyword, you are prompted once at the beginning of the deletion process to confirm the deletion.

If you use the **/recursive** keyword without the **/force** keyword, you are prompted to confirm the deletion of every file.

The prompting behavior depends on the setting of the **file prompt** global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, see the *Cisco IOS Command Reference for Release 12.1*.

---

## Examples

This example shows how to remove the directory that contains the old software image after a successful download of a new image:

```
Switch# delete /force /recursive flash:/old-image
```

You can verify that the directory was removed by entering the **dir filesystem:** privileged EXEC command.

---

## Related Commands

Command	Description
<a href="#">archive download-sw</a>	Downloads a new image to the switch and overwrites or keeps the existing image.

---

# deny (ARP access-list configuration)

Use the **deny** Address Resolution Protocol (ARP) access-list configuration command to deny an ARP packet based on matches against the DHCP bindings. Use the **no** form of this command to remove the specified access control entry (ACE) from the access list.

```
deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

```
no deny {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

## Syntax Description

<b>request</b>	(Optional) Define a match for the ARP request. When <b>request</b> is not specified, matching is performed against all ARP packets.
<b>ip</b>	Specify the sender IP address.
<b>any</b>	Deny any IP or MAC address.
<b>host sender-ip</b>	Deny the specified sender IP address.
<b>sender-ip sender-ip-mask</b>	Deny the specified range of sender IP addresses.
<b>mac</b>	Deny the sender MAC address.
<b>host sender-mac</b>	Deny a specific sender MAC address.
<b>sender-mac</b>	Deny the specified range of sender MAC addresses.
<b>sender-mac-mask</b>	
<b>response ip</b>	Define the IP address values for the ARP responses.
<b>host target-ip</b>	Deny the specified target IP address.
<b>target-ip target-ip-mask</b>	Deny the specified range of target IP addresses.
<b>mac</b>	Deny the MAC address values for the ARP responses.
<b>host target-mac</b>	Deny the specified target MAC address.
<b>target-mac</b>	Deny the specified range of target MAC addresses.
<b>target-mac-mask</b>	
<b>log</b>	(Optional) Log a packet when it matches the ACE.

## Defaults

There are no default settings. However, at the end of the ARP access list, there is an implicit **deny ip any mac any** command.

## Command Modes

ARP access-list configuration

## Command History

## Usage Guidelines

You can add deny clauses to drop ARP packets based on matching criteria.

**■ deny (ARP access-list configuration)****Examples**

This example shows how to define an ARP access list and to deny both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# deny ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>arp access-list</b></a>	Defines an ARP access control list (ACL).
<a href="#"><b>ip arp inspection filter vlan</b></a>	Permits ARP requests and responses from a host configured with a static IP address.
<a href="#"><b>permit (ARP access-list configuration)</b></a>	Permits an ARP packet based on matches against the DHCP bindings.
<a href="#"><b>show arp access-list</b></a>	Displays detailed information about ARP access lists.

# deny (MAC access-list configuration)

Use the **deny** MAC access-list configuration command to prevent non-IP traffic from being forwarded if the conditions are matched. Use the **no** form of this command to remove a deny condition from the named MAC access list.

```
{deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]

no {deny | permit} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | aarp | amber | cos cos | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```

## Syntax Description

<b>any</b>	Keyword to specify to deny any source or destination MAC address.
<b>host src MAC-addr   src-MAC-addr mask</b>	Define a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
<b>host dst-MAC-addr   dst-MAC-addr mask</b>	Define a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<b>type mask</b>	(Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.  The <i>type</i> is 0 to 65535, specified in hexadecimal.  The <i>mask</i> is a mask of <i>don't care</i> bits applied to the Ethertype before testing for a match.
<b>aarp</b>	(Optional) Select EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
<b>amber</b>	(Optional) Select EtherType DEC-Amber.
<b>cos cos</b>	(Optional) Select a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the <b>cos</b> option is configured.
<b>dec-spanning</b>	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
<b>decnet-iv</b>	(Optional) Select EtherType DECnet Phase IV protocol.
<b>diagnostic</b>	(Optional) Select EtherType DEC-Diagnostic.
<b>dsm</b>	(Optional) Select EtherType DEC-DSM.
<b>etype-6000</b>	(Optional) Select EtherType 0x6000.
<b>etype-8042</b>	(Optional) Select EtherType 0x8042.
<b>lat</b>	(Optional) Select EtherType DEC-LAT.
<b>lavc-sca</b>	(Optional) Select EtherType DEC-LAVC-SCA.

**■ deny (MAC access-list configuration)**

<b>lsap</b> <i>lsap-number mask</i>	(Optional) Use the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. <i>mask</i> is a mask of <i>don't care</i> bits applied to the LSAP number before testing for a match.
<b>mop-console</b>	(Optional) Select EtherType DEC-MOP Remote Console.
<b>mop-dump</b>	(Optional) Select EtherType DEC-MOP Dump.
<b>msdos</b>	(Optional) Select EtherType DEC-MSDOS.
<b>mumps</b>	(Optional) Select EtherType DEC-MUMPS.
<b>netbios</b>	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
<b>vines-echo</b>	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Select EtherType VINES IP.
<b>xns-idp</b>	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.

**Note**

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in [Table 2-12](#).

**Table 1-12 IPX Filtering Criteria**

<b>IPX Encapsulation Type</b>		<b>Filter Criterion</b>
<b>Cisco IOS Name</b>	<b>Novel Name</b>	
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

**Defaults**

This command has no defaults. However; the default action for a MAC-named ACL is to deny.

**Command Modes**

MAC-access list configuration

**Command History****Usage Guidelines**

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

For more information about named MAC extended access lists, see the software configuration guide for this release.

## Examples

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">mac access-list extended</a>	Creates an access list based on MAC addresses for non-IP traffic.
<a href="#">permit (MAC access-list configuration)</a>	Permits non-IP traffic to be forwarded if conditions are matched.
<a href="#">show access-lists</a>	Displays access control lists configured on a switch.

**■ diagnostic monitor**

# diagnostic monitor

Use the **diagnostic monitor** global configuration command to configure the health-monitoring diagnostic testing. Use the **no** form of this command to disable testing and return to the default settings.

```
diagnostic monitor test {test-id | test-id-range | all}
diagnostic monitor interval test {test-id | test-id-range | all} hh:mm:ss milliseconds day
diagnostic monitor syslog
diagnostic monitor threshold test {test-id | test-id-range | all} count failure count
no diagnostic monitor test {test-id | test-id-range | all}
no diagnostic monitor interval test {test-id | test-id-range | all}
no diagnostic monitor syslog
no diagnostic monitor threshold test {test-id | test-id-range | all} failure count
```

Syntax Description	
<b>test</b>	Specify a test to run.
<i>test-id</i>	Identification number for the test to be run; see the “Usage Guidelines” section for additional information.
<i>test-id-range</i>	Range of identification numbers for tests to be run; see the “Usage Guidelines” section for additional information.
<b>all</b>	Run all the diagnostic tests.
<b>interval</b>	Specify an interval between tests to be run.
<i>hh:mm:ss</i>	Specify the number of time between tests; see the “Usage Guidelines” section for formatting guidelines.
<i>milliseconds</i>	Specify the time in milliseconds; valid values are 0 to 999.
<i>day</i>	Specify the number of days between tests; see the “Usage Guidelines” section for formatting guidelines.
<b>syslog</b>	Enable the generation of a syslog message when a health-monitoring test fails.
<b>threshold</b>	Specify the failure threshold.
<b>failure count</b>	Specify the failure threshold count.
<i>count</i>	

**Defaults**

- Monitoring is disabled.
- **syslog** is enabled.

**Command Modes**

Global configuration

**Command History****Usage Guidelines**

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** privileged EXEC command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh*—Enter the hours from 0 to 23.
- *mm*—Enter the minutes from 0 to 60.
- *ss*—Enter the seconds from 0 to 60.
- *milliseconds*—Enter the milliseconds from 0 to 999.
- *day*—Enter the day as a number from 0 to 20.

When entering the **diagnostic monitor test {test-id|test-id-range|all}** command, follow these required guidelines

- Isolate network traffic by disabling all connected ports, and do not pump test packets during the test.
- Reset the system or the test module before putting the system back into the normal operating mode.

**Examples**

This example shows how to configure the specified test to run every 2 minutes:

```
Switch(config)# diagnostic monitor interval test 1 00:02:00 0 1
```

This example shows how to enable generating a syslog message when any health monitoring test fails:

```
Switch(config)# diagnostic monitor syslog
```

**Related Commands**

Command	Description
<b>show diagnostic</b>	Displays online diagnostic test results.

**■ diagnostic schedule**

# diagnostic schedule

Use the **diagnostic schedule** privileged EXEC command to configure the scheduling of diagnostic testing. Use the **no** form of this command to remove the scheduling and return to the default setting.

```
diagnostic schedule test {test-id | test-id-range | all | basic | non-disruptive} {daily hh:mm |
on mm dd yyyy hh:mm | weekly day-of-week hh:mm}
```

```
no diagnostic schedule test {test-id | test-id-range | all | basic | non-disruptive} {daily hh:mm |
on mm dd yyyy hh:mm | weekly day-of-week hh:mm}
```

Syntax Description	
<b>test</b>	Specify the test to be scheduled.
<i>test-id</i>	Identification number for the test to be run; see the “Usage Guidelines” section for additional information.
<i>test-id-range</i>	Range of identification numbers for tests to be run; see the “Usage Guidelines” section for additional information.
<b>all</b>	Run all diagnostic tests.
<b>basic</b>	Run basic on-demand diagnostic tests.
<b>non-disruptive</b>	Run the nondisruptive health-monitoring tests.
<b>daily hh:mm</b>	Specify the daily scheduling of a test-based diagnostic task; see the “Usage Guidelines” section for formatting guidelines.
<b>on mm dd yyyy hh:mm</b>	Specify the scheduling of a test-based diagnostic task; see the “Usage Guidelines” section for formatting guidelines.
<b>weekly day-of-week hh:mm</b>	Specify the weekly scheduling of a test-based diagnostic task; see the “Usage Guidelines” section for formatting guidelines.

<b>Defaults</b>	This command has no default settings.
<b>Command Modes</b>	Global configuration
<b>Command History</b>	

**Usage Guidelines**

Use these guidelines when scheduling testing:

- *test-id*—Enter the **show diagnostic content** command to display the test ID list.
- *test-id-range*—Enter the **show diagnostic content** command to display the test ID list. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).
- *hh:mm*—Enter the time as a 2-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required.
- *mm*—Spell out the month, such as January, February... December (either upper case or lower case characters).
- *dd*—Enter the day as a 2-digit number.
- *yyyy*—Enter the year as a 4-digit number.
- *day-of-week*—Spell out the day of the week, such as Monday, Tuesday... Sunday (either upper case or lower case characters).

**Examples**

This example shows how to schedule diagnostic testing on a specific date and time for a specific switch:

```
Switch(config)# diagnostic schedule test 1,2,4-6 on january 3 2006 23:32
```

This example shows how to schedule diagnostic testing to occur weekly at a certain time:

```
Switch(config)# diagnostic schedule test 1,2,4-6 weekly friday 09:23
```

**Related Commands**

Command	Description
<b>show diagnostic</b>	Displays online diagnostic test results.

**■ diagnostic start**

# diagnostic start

Use the **diagnostic start** user command to run the specified diagnostic test.

**diagnostic start test {test-id | test-id-range | all | basic | non-disruptive}**

---

## Syntax Description

<b>test</b>	Specify a test to run.
<i>test-id</i>	Identification number for the test to be run; see the “Usage Guidelines” section for additional information.
<i>test-id-range</i>	Range of identification numbers for tests to be run; see the “Usage Guidelines” section for additional information.
<b>all</b>	Run all diagnostic tests.
<b>basic</b>	Run basic on-demand diagnostic tests.
<b>non-disruptive</b>	Run the nondisruptive health-monitoring tests.

---



---

## Defaults

This command has no default settings.

---

## Command Modes

User EXEC

---

## Command History

---

### Usage Guidelines

Enter the **show diagnostic content** command to display the test ID list.

Enter the *test-id-range* as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).

---

## Examples

---

## Related Commands

Command	Description
<a href="#">show diagnostic</a>	Displays online diagnostic test results.

---

# dot1x

Use the **dot1x** global configuration command to globally enable IEEE 802.1x authentication. Use the **no** form of this command to return to the default setting.

```
dot1x {critical {eapol | recovery delay milliseconds} | {guest-vlan supplicant} | system-auth-control}
```

```
no dot1x {critical {eapol | recovery delay} | {guest-vlan supplicant} | system-auth-control}
```



Though visible in the command-line help strings, the **credentials name** keywords are not supported.

## Syntax Description

<b>critical {eapol   recovery delay milliseconds}</b>	Configure the inaccessible authentication bypass parameters. For more information, see the <a href="#">dot1x critical (global configuration)</a> command.
<b>guest-vlan supplicant</b>	Enable optional guest VLAN behavior globally on the switch.
<b>system-auth-control</b>	Enable IEEE 802.1x authentication globally on the switch.

## Defaults

IEEE 802.1x authentication is disabled, and the optional guest VLAN behavior is disabled.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

You must enable authentication, authorization, and accounting (AAA) and specify the authentication method list before globally enabling IEEE 802.1x authentication. A method list describes the sequence and authentication methods to be used to authenticate a user.

Before globally enabling IEEE 802.1x authentication on a switch, remove the EtherChannel configuration from the interfaces on which IEEE 802.1x authentication and EtherChannel are configured.

If you are using a device running the Cisco Access Control Server (ACS) application for IEEE 802.1x authentication with EAP-Transparent LAN Services (TLS) and with EAP-MD5, make sure that the device is running ACS Version 3.2.1 or later.

You can use the **guest-vlan supplicant** keywords to enable the optional IEEE 802.1x guest VLAN behavior globally on the switch. For more information, see the [dot1x guest-vlan](#) command.

## Examples

This example shows how to globally enable IEEE 802.1x authentication on a switch:

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

This example shows how to globally enable the optional guest VLAN behavior on a switch:

```
Switch(config)# dot1x guest-vlan supplicant
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>dot1x critical (global configuration)</b></a>	Configures the parameters for the inaccessible authentication bypass feature on the switch.
<a href="#"><b>dot1x guest-vlan</b></a>	Enables and specifies an active VLAN as an IEEE 802.1x guest VLAN.
<a href="#"><b>dot1x port-control</b></a>	Enables manual control of the authorization state of the port.
<a href="#"><b>show dot1x [interface <i>interface-id</i>]</b></a>	Displays IEEE 802.1x status for the specified port.

# dot1x auth-fail max-attempts

Use the **dot1x auth-fail max-attempts** interface configuration command to configure the maximum allowable authentication attempts before a port is moved to the restricted VLAN. To return to the default setting, use the **no** form of this command.

**dot1x auth-fail max-attempts** *max-attempts*

**no dot1x auth-fail max-attempts**

<b>Syntax Description</b>	<i>max-attempts</i>	Specify a maximum number of authentication attempts allowed before a port is moved to the restricted VLAN. The range is 1 to 3, the default value is 3.
---------------------------	---------------------	---

<b>Defaults</b>	The default value is 3 attempts.
-----------------	----------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SED	This command was introduced.

<b>Usage Guidelines</b>	If you reconfigure the maximum number of authentication attempts allowed by the VLAN, the change takes effect after the re-authentication timer expires.
-------------------------	--

<b>Examples</b>	This example shows how to set 2 as the maximum number of authentication attempts allowed before the port is moved to the restricted VLAN on port 3:
-----------------	---

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

To verify your settings, ether the **show dot1x [interface *interface-id*]** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x auth-fail vlan</b> [ <i>vlan id</i> ]	Enables the optional restricted VLAN feature.
	<b>dot1x max-reauth-req</b> [ <i>count</i> ]	Sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.
	<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

dot1x auth-fail vlan

## dot1x auth-fail vlan

Use the **dot1x auth-fail vlan** interface configuration command to enable the restricted VLAN on a port. To return to the default setting, use the **no** form of this command.

**dot1x auth-fail vlan *vlan-id***

**no dot1x auth-fail vlan**

<b>Syntax Description</b>	<i>vlan-id</i> Specify a VLAN in the range of 1 to 4094.
---------------------------	--

<b>Defaults</b>	No restricted VLAN is configured.
-----------------	-----------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SED	This command was introduced.

<b>Usage Guidelines</b>	You can configure a restricted VLAN on ports configured as follows:
-------------------------	---

- single-host (default) mode
- auto mode for authorization

You should enable re-authentication. The ports in restricted VLANs do not receive re-authentication requests if it is disabled. To start the re-authentication process, the restricted VLAN must receive a link-down event or an Extensible Authentication Protocol (EAP) logoff event from the port. If a host is connected through a hub, the port might never receive a link-down event when that host is disconnected, and, as a result, might not detect any new hosts until the next re-authentication attempt occurs.

If the supplicant fails authentication, the port is moved to a restricted VLAN, and an EAP *success* message is sent to the supplicant. Because the supplicant is not notified of the actual authentication failure, there might be confusion about this restricted network access. An EAP success message is sent for these reasons:

- If the EAP success message is not sent, the supplicant tries to authenticate every 60 seconds (the default) by sending an EAP-start message.
- Some hosts (for example, devices running Windows XP) cannot implement DHCP until they receive an EAP success message.

A supplicant might cache an incorrect username and password combination after receiving an EAP success message from the authenticator and re-use that information in every re-authentication. Until the supplicant sends the correct username and password combination, the port remains in the restricted VLAN.

Internal VLANs used for Layer 3 ports cannot be configured as restricted VLANs.

You cannot configure a VLAN to be both a restricted VLAN and a voice VLAN. If you do this, a syslog message is generated.

When a restricted VLAN port is moved to an unauthorized state, the authentication process restarts. If the supplicant fails the authentication process again, the authenticator waits in the held state. After the supplicant has correctly re-authenticated, all IEEE 802.1x ports are reinitialized and treated as normal IEEE 802.1x ports.

When you reconfigure a restricted VLAN as a different VLAN, any ports in the restricted VLAN are also moved, and the ports stay in their currently authorized state.

When you shut down or remove a restricted VLAN from the VLAN database, any ports in the restricted VLAN are immediately moved to an unauthorized state, and the authentication process restarts. The authenticator does not wait in a held state because the restricted VLAN configuration still exists. While the restricted VLAN is inactive, all authentication attempts are counted so that when the restricted VLAN becomes active, the port is immediately placed in the restricted VLAN.

The restricted VLAN is supported only in single host mode (the default port mode). For this reason, when a port is placed in a restricted VLAN, the supplicant's MAC address is added to the MAC address table, and any other MAC address that appears on the port is treated as a security violation.

## Examples

This example shows how to configure a restricted VLAN on port 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch#
```

You can verify your configuration by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

## Related Commands

Command	Description
<b>dot1x auth-fail max-attempts</b> [ <i>max-attempts</i> ]	Configures the number of authentication attempts allowed before assigning a supplicant to the restricted VLAN.
<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

**dot1x control-direction**

# dot1x control-direction

This is an obsolete command.

Use the **dot1x control-direction** interface configuration command to enable the IEEE 802.1x authentication with the wake-on-LAN (WoL) feature and to configure the port control as unidirectional or bidirectional. Use the **no** form of this command to return to the default setting.

**dot1x control-direction {both | in}**

**no dot1x control-direction**

<b>Syntax Description</b>	<b>both</b>	Enable bidirectional control on port. The port cannot receive packets from or send packets to the host.
	<b>in</b>	Enable unidirectional control on port. The port can send packets to the host but cannot receive packets from the host.

**Defaults** The port is in bidirectional mode.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(58)SE	The <b>dot1x control-direction</b> interface configuration command was replaced by the <b>authentication control-direction</b> interface configuration command.

**Usage Guidelines** Use the **both** keyword or the **no** form of this command to return to the default setting, bidirectional mode.

For more information about WoL, see the “Using IEEE 802.1x Authentication with Wake-on-LAN” section in the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the software configuration guide.

**Examples** This example shows how to enable unidirectional control:

```
Switch(config-if)# dot1x control-direction in
```

This example shows how to enable bidirectional control:

```
Switch(config-if)# dot1x control-direction both
```

You can verify your settings by entering the **show dot1x all** privileged EXEC command.

The **show dot1x all** privileged EXEC command output is the same for all switches except for the port names and the state of the port. If a host is attached to the port but is not yet authenticated, a display similar to this appears:

```
Suplicant MAC 0002.b39a.9275
```

```

AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED

```

If you enter the **dot1x control-direction in** interface configuration command to enable unidirectional control, this appears in the **show dot1x all** command output:

```
ControlDirection = In
```

If you enter the **dot1x control-direction in** interface configuration command and the port cannot support this mode due to a configuration conflict, this appears in the **show dot1x all** command output:

```
ControlDirection = In (Disabled due to port settings)
```

Related Commands	Command	Description
	authentication control-direction	Enable the IEEE 802.1x authentication with the wake-on-LAN (WoL) feature
	<b>show dot1x [all   interface <i>interface-id</i>]</b>	Displays control-direction port setting status for the specified interface.

---

**dot1x credentials (global configuration)**

# dot1x credentials (global configuration)

Use the **dot1x credentials** global configuration command to configure a profile on a supplicant switch.

**dot1x credentials *profile***

**no dot1x credentials *profile***

<b>Syntax Description</b>	<i>profile</i> Specify a profile for the supplicant switch.
---------------------------	---

<b>Defaults</b>	No profile is configured for the switch.
-----------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	You must have another switch set up as the authenticator for this switch to be the supplicant.
-------------------------	--

<b>Examples</b>	This example shows how to configure a switch as a supplicant:
-----------------	---

```
Switch(config)# dot1x credentials profile
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cisp enable</b>	Enables Client Information Signalling Protocol (CISP).
	<b>show cisp</b>	Displays CISP information for a specified interface.

# dot1x critical (global configuration)

Use the **dot1x critical** global configuration command to configure the parameters for the inaccessible authentication bypass feature, also referred to as critical authentication or the authentication, authorization, and accounting (AAA) fail policy. To return to default settings, use the **no** form of this command.

**dot1x critical {eapol | recovery delay milliseconds}**

**no dot1x critical {eapol | recovery delay}**

<b>Syntax Description</b>	<b>eapol</b> Specify that the switch sends an EAPOL-Success message when the switch puts the critical port in the critical-authentication state. <b>recovery delay milliseconds</b> Set the recovery delay period in milliseconds. The range is from 1 to 10000 milliseconds.
---------------------------	--

<b>Defaults</b>	The switch does not send an EAPOL-Success message to the host when the switch successfully authenticates the critical port by putting the critical port in the critical-authentication state.  The recovery delay period is 1000 milliseconds (1 second).
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>eapol</b> keyword to specify that the switch sends an EAPOL-Success message when the switch puts the critical port in the critical-authentication state.  Use the <b>recovery delay milliseconds</b> keyword to set the recovery delay period during which the switch waits to re-initialize a critical port when a RADIUS server that was unavailable becomes available. The default recovery delay period is 1000 milliseconds. A port can be re-initialized every second.  To enable inaccessible authentication bypass on a port, use the <b>dot1x critical</b> interface configuration command. To configure the access VLAN to which the switch assigns a critical port, use the <b>dot1x critical vlan vlan-id</b> interface configuration command.
-------------------------	---

<b>Examples</b>	This example shows how to set 200 as the recovery delay period on the switch: <pre>Switch# dot1x critical recovery delay 200</pre> You can verify your configuration by entering the <b>show dot1x</b> privileged EXEC command.
-----------------	--

**dot1x critical (global configuration)**

Related Commands	Command	Description
	<a href="#">dot1x critical (interface configuration)</a>	Enables the inaccessible authentication bypass feature, and configures the access VLAN for the feature.
	<a href="#">show dot1x</a>	Displays IEEE 802.1x status for the specified port.

# dot1x critical (interface configuration)

Use the **dot1x critical** interface configuration command to enable the inaccessible-authentication-bypass feature, also referred to as critical authentication or the authentication, authorization, and accounting (AAA) fail policy. You can also configure the access VLAN to which the switch assigns the critical port when the port is in the critical-authentication state. To disable the feature or return to default, use the **no** form of this command.

**dot1x critical [recovery action reinitialize | vlan *vlan-id*]**

**no dot1x critical [recovery | vlan]**

<b>Syntax Description</b>	<b>recovery action reinitialize</b> Enable the inaccessible-authentication-bypass recovery feature, and specify that the recovery action is to authenticate the port when an authentication server is available.
	<b>vlan <i>vlan-id</i></b> Specify the access VLAN to which the switch can assign a critical port. The range is from 1 to 4094.

## Defaults

The inaccessible-authentication-bypass feature is disabled.

The recovery action is not configured.

The access VLAN is not configured.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

To specify the access VLAN to which the switch assigns a critical port when the port is in the critical-authentication state, use the **vlan *vlan-id*** keywords. The specified type of VLAN must match the type of port, as follows:

- If the critical port is an access port, the VLAN must be an access VLAN.
- If the critical port is a private VLAN host port, the VLAN must be a secondary private VLAN.
- If the critical port is a routed port, you can specify a VLAN, but this is optional.

If the client is running Windows XP and the critical port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.

If the Windows XP client is configured for DHCP and has an IP address from the DHCP server, receiving an EAP-Success message on a critical port might not re-initiate the DHCP configuration process.

You can configure the inaccessible authentication bypass feature and the restricted VLAN on an IEEE 802.1x port. If the switch tries to re-authenticate a critical port in a restricted VLAN and all the RADIUS servers are unavailable, the switch changes the port state to the critical authentication state, and it remains in the restricted VLAN.

You can configure the inaccessible bypass feature and port security on the same switch port.

## dot1x critical (interface configuration)

### Examples

This example shows how to enable the inaccessible authentication bypass feature on a port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# dot1x critical
Switch(config-if)# end
Switch(config)# end
Switch#
```

You can verify your configuration by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

### Related Commands

Command	Description
<a href="#">dot1x critical (global configuration)</a>	Configures the parameters for the inaccessible authentication bypass feature on the switch.
<a href="#">show dot1x [interface <i>interface-id</i>]</a>	Displays IEEE 802.1x status for the specified port.

# dot1x default

Use the **dot1x default** interface configuration command to reset the IEEE 802.1x parameters to their default values.

## dot1x default

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

### Defaults

These are the default values:

- The per-port IEEE 802.1x protocol enable state is disabled (force-authorized).
- The number of seconds between re-authentication attempts is 3600 seconds.
- The periodic re-authentication is disabled.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The host mode is single host.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

### Command Modes

Interface configuration

### Command History

#### Examples

This example shows how to reset the IEEE 802.1x parameters on a port:

```
Switch(config-if)# dot1x default
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

### Related Commands

Command	Description
<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

**dot1x fallback**

# dot1x fallback

Use the **dot1xfallback** interface configuration command to configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. To return to the default setting, use the **no** form of this command.

**dot1x fallback *profile***

**no dot1x fallback**

<b>Syntax Description</b>	<i>profile</i>	Specify a fallback profile for clients that do not support IEEE 802.1x authentication.
---------------------------	----------------	--

<b>Defaults</b>	No fallback is enabled.
-----------------	-------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(35)SE	This command was introduced.

<b>Usage Guidelines</b>	You must enter the <b>dot1x port-control auto</b> interface configuration command on a switch port before entering this command.
-------------------------	--

<b>Examples</b>	This example shows how to specify a fallback profile to a switch port that has been configured for IEEE 802.1x authentication:
-----------------	--

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show dot1x [interface <i>interface-id</i>]</a>	Displays IEEE 802.1x status for the specified port.
	<a href="#">fallback profile</a>	Create a web authentication fallback profile.
	<a href="#">ip admission</a>	Enable web authentication on a port
	<a href="#">ip admission name proxy http</a>	Enable web authentication globally on a switch

# dot1x guest-vlan

Use the **dot1x guest-vlan** interface configuration command to specify an active VLAN as an IEEE 802.1x guest VLAN. Use the **no** form of this command to return to the default setting.

**dot1x guest-vlan *vlan-id***

**no dot1x guest-vlan**

<b>Syntax Description</b>	<i>vlan-id</i> Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094.
---------------------------	---

<b>Defaults</b>	No guest VLAN is configured.
-----------------	------------------------------

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

## Command History

You can configure a guest VLAN on one of these switch ports:

- A static-access port that belongs to a nonprivate VLAN.
- A private-VLAN port that belongs to a secondary private VLAN. All the hosts connected to the switch port are assigned to private VLANs, whether or not the posture validation was successful. The switch determines the primary private VLAN by using the primary- and secondary-private-VLAN associations on the switch.

For each IEEE 802.1x port on the switch, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the switch) not running IEEE 802.1x authentication. These users might be upgrading their systems for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x-capable.

When you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

The switch maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is reset upon loss of link.

Any number of non-IEEE 802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x ports in single-host or multiple-hosts mode.

You can configure any active VLAN except an Remote Switched Port Analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on trunk ports; it is supported only on access ports.

**dot1x guest-vlan**

After you configure a guest VLAN for an IEEE 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the IEEE 802.1x authentication process (**dot1x timeout quiet-period** and **dot1x timeout tx-period** interface configuration commands). The amount to decrease the settings depends on the connected IEEE 802.1x client type.

The switch supports *MAC authentication bypass*. When it is enabled on an IEEE 802.1x port, the switch can authorize clients based on the client MAC address when IEEE 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an IEEE 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is specified. For more information, see the “Using IEEE 802.1x Authentication with MAC Authentication Bypass” section in the “Configuring IEEE 802.1x Port-Based Authentication” chapter of the software configuration guide.

**Examples**

This example shows how to specify VLAN 5 as an IEEE 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 5
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an IEEE 802.1x guest VLAN when an IEEE 802.1x port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

This example shows how to enable the optional guest VLAN behavior and to specify VLAN 5 as an IEEE 802.1x guest VLAN:

```
Switch(config)# dot1x guest-vlan supplicant
Switch(config-if)# dot1x guest-vlan 5
```

You can verify your settings by entering the **show dot1x [interface interface-id]** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>dot1x</b>	Enables the optional guest VLAN supplicant feature.
<b>show dot1x [interface interface-id]</b>	Displays IEEE 802.1x status for the specified port.

# dot1x host-mode

Use the **dot1x host-mode** interface configuration command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port. Use the **multi-domain** keyword to enable multidomain authentication (MDA) on an IEEE 802.1x-authorized port. Use the **no** form of this command to return to the default setting.

**dot1x host-mode {multi-host | single-host | multi-domain}**

**no dot1x host-mode [multi-host | single-host | multi-domain]**

<b>Syntax Description</b>	<b>multi-host</b> Enable multiple-hosts mode on the switch. <b>single-host</b> Enable single-host mode on the switch. <b>multi-domain</b> Enable MDA on a switch port.
---------------------------	--

**Defaults**      The default is single-host mode.

**Command Modes**      Interface configuration

## Command History

**Usage Guidelines**      Use this command to limit an IEEE 802.1x-enabled port to a single client or to attach multiple clients to an IEEE 802.1x-enabled port. In multiple-hosts mode, only one of the attached hosts needs to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **multi-domain** keyword to enable MDA on a port. MDA divides the port into both a data domain and a voice domain. MDA allows both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), on the same IEEE 802.1x-enabled port.

Before entering this command, make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified port.

## Examples

This example shows how to enable IEEE 802.1x authentication globally, to enable IEEE 802.1x authentication on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

This example shows how to globally enable IEEE 802.1x authentication, to enable IEEE 802.1x authentication, and to enable MDA on the specified port:

```
Switch(config)# dot1x system-auth-control
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
```

**dot1x host-mode**

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

**Related Commands**

Command	Description
<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

# dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return the specified IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the port.

**dot1x initialize [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Port to be initialized.				
<b>Defaults</b>	There is no default setting.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>					
<b>Usage Guidelines</b>	Use this command to initialize the IEEE 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized. There is not a <b>no</b> form of this command.				
<b>Examples</b>	This example shows how to manually initialize a port:  You can verify the unauthorized port status by entering the <b>show dot1x [interface <i>interface-id</i>]</b> privileged EXEC command.				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><a href="#">show dot1x [interface <i>interface-id</i>]</a></td><td>Displays IEEE 802.1x status for the specified port.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">show dot1x [interface <i>interface-id</i>]</a>	Displays IEEE 802.1x status for the specified port.
<b>Command</b>	<b>Description</b>				
<a href="#">show dot1x [interface <i>interface-id</i>]</a>	Displays IEEE 802.1x status for the specified port.				

dot1x mac-auth-bypass

## dot1x mac-auth-bypass

Use the **dot1x mac-auth-bypass** interface configuration command to enable the MAC authentication bypass feature. Use the **no** form of this command to disable MAC authentication bypass feature.

**dot1x mac-auth-bypass [eap | timeout inactivity *value*]**

**no dot1x mac-auth-bypass**

<b>Syntax Description</b>	<b>eap</b> (Optional) Configure the switch to use Extensible Authentication Protocol (EAP) for authentication. <b>timeout inactivity <i>value</i></b> (Optional) Configure the number of seconds that a connected host can be inactive before it is placed in an unauthorized state. The range is 1 to 65535.
---------------------------	--

**Defaults** MAC authentication bypass is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(25)SEE	This command was introduced.
	12.2(35)SE	The <b>timeout inactivity <i>value</i></b> keywords were added.

<b>Usage Guidelines</b>	Unless otherwise stated, the MAC authentication bypass usage guidelines are the same as the IEEE 802.1x authentication guidelines.  If you disable MAC authentication bypass from a port after the port has been authenticated with its MAC address, the port state is not affected.  If the port is in the unauthorized state and the client MAC address is not the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.  If the port is in the authorized state, the port remains in this state until re-authorization occurs.  If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an IEEE 802.1x-capable supplicant and uses IEEE 802.1x authentication (not MAC authentication bypass) to authorize the interface.  Clients that were authorized with MAC authentication bypass can be re-authenticated.  For more information about how MAC authentication bypass and IEEE 802.1x authentication interact, see the “Understanding IEEE 802.1x Authentication with MAC Authentication Bypass” section and the “IEEE 802.1x Authentication Configuration Guidelines” section in the “Configuring IEEE 802.1x Port-Based Authentication” chapter of the software configuration guide.
-------------------------	---

**Examples**

This example shows how to enable MAC authentication bypass and to configure the switch to use EAP for authentication:

```
Switch(config-if)# dot1x mac-auth-bypass eap
```

This example shows how to enable MAC authentication bypass and to configure the timeout if the connected host is inactive for 30 seconds:

```
Switch(config-if)# dot1x mac-auth-bypass timeout inactivity 30
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

**Related Commands**

Command	Description
<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

**dot1x max-reauth-req**

Use the **dot1x max-reauth-req** interface configuration command to set the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state. Use the **no** form of this command to return to the default setting.

**dot1x max-reauth-req count**

**no dot1x max-reauth-req**

Syntax Description	count	Sets the number of times that switch retransmits EAPOL-Identity-Request frames to start the authentication process before the port changes to the unauthorized state. If a non-802.1x capable device is connected to a port, the switch retries two authentication attempts by default. If a guest VLAN is configured on the port, after two re-authentication attempts, the port is authorized on the guest vlan by default. The range is 1 to 10. The default is 2.
--------------------	-------	---

**Defaults**

The default is 2 times.

**Command Modes**

Interface configuration

**Command History****Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Examples**

This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port changes to the unauthorized state:

```
Switch(config-if)# dot1x max-reauth-req 4
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

Related Commands	Command	Description
	<b>dot1x max-req</b>	Sets the maximum number of times that the switch forwards an EAP frame (assuming that no response is received) to the authentication server before restarting the authentication process.
	<b>dot1x timeout tx-period</b>	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request.
	<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

**dot1x max-req**

# dot1x max-req

Use the **dot1x max-req** interface configuration command to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) frame from the authentication server (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to return to the default setting.

**dot1x max-req count**

**no dot1x max-req**

---

<b>Syntax Description</b>	<b>count</b>	Number of times that the switch attempts to retransmit EAPOL DATA packets before restarting the authentication process. For example, if you have a supplicant in the middle of authentication process and a problem occurs, the authenticator will re-transmit data requests two times before stopping the process. The range is 1 to 10; the default is 2
---------------------------	--------------	--

---

<b>Defaults</b>	The default is 2 times.
-----------------	-------------------------

---

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

---

<b>Command History</b>	
<b>Usage Guidelines</b>	You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

---

<b>Examples</b>	This example shows how to set 5 as the number of times that the switch sends an EAP frame from the authentication server to the client before restarting the authentication process:
-----------------	--

```
Switch(config-if)# dot1x max-req 5
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x timeout tx-period</b>	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request.
	<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

---

# dot1x pae

Use the **dot1x pae** interface configuration command to configure the port as an IEEE 802.1x port access entity (PAE) authenticator. Use the **no** form of this command to disable IEEE 802.1x authentication on the port.

## **dot1x pae authenticator**

## **no dot1x pae**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	The port is not an IEEE 802.1x PAE authenticator, and IEEE 802.1x authentication is disabled on the port.
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>no dot1x pae</b> interface configuration command to disable IEEE 802.1x authentication on the port.
-------------------------	--

When you configure IEEE 802.1x authentication on a port, such as by entering the **dot1x port-control** interface configuration command, the switch automatically configures the port as an IEEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is disabled.

<b>Examples</b>	This example shows how to disable IEEE 802.1x authentication on the port:
-----------------	---

```
Switch(config-if)# no dot1x pae
```

You can verify your settings by entering the **show dot1x** or **show eap** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show dot1x</a>	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.
	<a href="#">show eap</a>	Displays EAP registration and session information for the switch or for the specified port.

**dot1x port-control**

# dot1x port-control

Use the **dot1x port-control** interface configuration command to enable manual control of the authorization state of the port. Use the **no** form of this command to return to the default setting.

**dot1x port-control {auto | force-authorized | force-unauthorized}**

**no dot1x port-control**

Syntax Description	auto	Enable IEEE 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange between the switch and the client.
	force-authorized	Disable IEEE 802.1x authentication on the port and cause the port to transition to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client.
	force-unauthorized	Deny all access through this port by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

**Defaults**

The default is force-authorized.

**Command Modes**

Interface configuration

**Command History****Usage Guidelines**

You must globally enable IEEE 802.1x authentication on the switch by using the **dot1x system-auth-control** global configuration command before enabling IEEE 802.1x authentication on a specific port.

You can use the **auto** keyword only if the port is not configured as one of these:

- Trunk port—if you try to enable IEEE 802.1x authentication on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.
- Dynamic ports—a port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x authentication on a dynamic port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
- Dynamic-access ports—if you try to enable IEEE 802.1x authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—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 or RSPAN destination. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

To globally disable IEEE 802.1x authentication on the switch, use the **no dot1x system-auth-control** global configuration command. To disable IEEE 802.1x authentication on a specific port or to return to the default setting, use the **no dot1x port-control** interface configuration command.

## Examples

This example shows how to enable IEEE 802.1x authentication on a port:

```
Switch(config-if)# dot1x port-control auto
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

## Related Commands

Command	Description
<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

---

dot1x re-authenticate

## dot1x re-authenticate

Use the **dot1x re-authenticate** privileged EXEC command to manually initiate a re-authentication of the specified IEEE 802.1x-enabled port.

**dot1x re-authenticate [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional)
---------------------------	---

<b>Defaults</b>	There is no default setting.
-----------------	------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.
-------------------------	---

<b>Examples</b>	This example shows how to manually re-authenticate the device connected to a port:
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">dot1x reauthentication</a>	Enables periodic re-authentication of the client.
	<a href="#">dot1x timeout reauth-period</a>	Sets the number of seconds between re-authentication attempts.

# dot1x reauthentication

Use the **dot1x reauthentication** interface configuration command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

**dot1x reauthentication**

**no dot1x reauthentication**

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

**Defaults** Periodic re-authentication is disabled.

**Command Modes** Interface configuration

## Command History

**Usage Guidelines** You configure the amount of time between periodic re-authentication attempts by using the **dot1x timeout reauth-period** interface configuration command.

**Examples** This example shows how to disable periodic re-authentication of the client:

```
Switch(config-if)# no dot1x reauthentication
```

This example shows how to enable periodic re-authentication and to set the number of seconds between re-authentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

## Related Commands

Command	Description
<a href="#">dot1x re-authenticate</a>	Manually initiates a re-authentication of all IEEE 802.1x-enabled ports.
<a href="#">dot1x timeout reauth-period</a>	Sets the number of seconds between re-authentication attempts.
<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

**dot1x supplicant controlled transient**

To control access to an 802.1x supplicant port during authentication, use the **dot1x supplicant controlled transient** command in global configuration mode. To open the supplicant port during authentication, use the **no** form of this command.

**dot1x supplicant controlled transient**

**no dot1x supplicant controlled transient**

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

**Defaults** Access is allowed to 802.1x supplicant ports during authentication.

**Command Modes** Global configuration

Command History	Release	Modification
	15.0(1)SE	This command was introduced.

**Usage Guidelines** In the default state, when you connect a supplicant switch to an authenticator switch that has BPCU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient** command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** cinterface configuration command.

If you globally enable BPDU guard on the authenticator switch by using the **spanning-tree portfast bpduguard default** global configuration command, entering the **dot1x supplicant controlled transient** command does not prevent the BPDU violation.

**Examples** This example shows how to control access to 802.1x supplicant ports on a switch during authentication:

```
Switch(config)# dot1x supplicant controlled transient
```

Related Commands	Command	Description
	<b>cisp enable</b>	Enables Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
	<b>dot1x credentials</b>	Configures the 802.1x supplicant credentials on the port.
	<b>dot1x pae supplicant</b>	Configures an interface to act only as a supplicant.

---

dot1x supplicant force-multicast

## dot1x supplicant force-multicast

Use the **dot1x supplicant force-multicast** global configuration command to force a supplicant switch to send *only* multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets. Use the **no** form of this command to return to the default setting.

**dot1x supplicant force-multicast**

**no dot1x supplicant force-multicast**

---

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

---

**Defaults**

The supplicant switch sends unicast EAPoL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

---



---

**Usage Guidelines** Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

---

**Examples** This example shows how force a supplicant switch to send multicast EAPOL packets to authenticator switch:

```
Switch(config)# dot1x supplicant force-multicast
```

---

Related Commands	Command	Description
	<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
	<b>dot1x credentials</b>	Configure the 802.1x supplicant credentials on the port.
	<b>dot1x pae supplicant</b>	Configure an interface to act only as a supplicant.

---

# dot1x test eapol-capable

Use the **dot1x test eapol-capable** privileged EXEC command to monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x.

**dot1x test eapol-capable [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Port to be queried.
---------------------------	---

<b>Defaults</b>	There is no default setting.
-----------------	------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)SE	This command was introduced.

<b>Usage Guidelines</b>	Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.
-------------------------	---

There is not a **no** form of this command.

<b>Examples</b>	This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:
-----------------	---

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet0/13 is EAPOL
capable
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x test timeout <i>timeout</i></b>	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

**dot1x test timeout**

## dot1x test timeout

Use the **dot1x test timeout** global configuration command to configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness.

**dot1x test timeout *timeout***

<b>Syntax Description</b>	<i>timeout</i>	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default setting is 10 seconds.
-----------------	------------------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)SE	This command was introduced.

<b>Usage Guidelines</b>	Use this command to configure the timeout used to wait for EAPOL response. There is not a <b>no</b> form of this command.
-------------------------	--

<b>Examples</b>	This example shows how to configure the switch to wait 27 seconds for an EAPOL response:
	Switch# <b>dot1x test timeout 27</b>

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dot1x test eapol-capable [interface <i>interface-id</i>]</b>	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

# dot1x timeout

Use the **dot1x timeout** interface configuration command to set IEEE 802.1x timers. Use the **no** form of this command to return to the default setting.

```
dot1x timeout {quiet-period seconds | ratelimit-period seconds | reauth-period {seconds | server} | server-timeout seconds | supp-timeout seconds | tx-period seconds}
```

```
no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}
```

Syntax Description	
<b>quiet-period</b> <i>seconds</i>	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535.
<b>ratelimit-period</b> <i>seconds</i>	Number of seconds that the switch ignores Extensible Authentication Protocol over LAN (EAPOL) packets from clients that have been successfully authenticated during this duration. The range is 1 to 65535.
<b>reauth-period {seconds   server}</b>	<p>Set the number of seconds between re-authentication attempts.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <i>seconds</i>—Sets the number of seconds from 1 to 65535; the default is 3600 seconds.</li> <li>• <b>server</b>—Sets the number of seconds as the value of the Session-Timeout RADIUS attribute (Attribute[27]).</li> </ul>
<b>server-timeout</b> <i>seconds</i>	<p>Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server.</p> <p>The range is 1 to 65535. However, we recommend a minimum setting of 30.</p>
<b>supp-timeout</b> <i>seconds</i>	Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client. The range is 30 to 65535.
<b>tx-period</b> <i>seconds</i>	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535.

## Defaults

These are the default settings:

- reauth-period** is 3600 seconds.
- quiet-period** is 60 seconds.
- tx-period** is 5 seconds.
- supp-timeout** is 30 seconds.
- server-timeout** is 30 seconds.
- rate-limit** is 1 second.

## Command Modes

Interface configuration

**dot1x timeout****Command History**

<b>Release</b>	<b>Modification</b>
12.2(25)SEE	The <b>ratelimit-period</b> keyword was introduced.
12.2(40)SE	The range for <b>tx-period seconds</b> is incorrect. The correct range is from 1 to 65535.

**Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

**Examples**

This example shows how to enable periodic re-authentication and to set 4000 as the number of seconds between re-authentication attempts:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

This example shows how to enable periodic re-authentication and to specify the value of the Session-Timeout RADIUS attribute as the number of seconds between re-authentication attempts:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

This example shows how to set 30 seconds as the quiet time on the switch:

```
Switch(config-if)# dot1x timeout quiet-period 30
```

This example shows how to set 45 seconds as the switch-to-authentication server retransmission time:

```
Switch(config)# dot1x timeout server-timeout 45
```

This example shows how to set 45 seconds as the switch-to-client retransmission time for the EAP request frame:

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

This example shows how to set 60 as the number of seconds to wait for a response to an EAP-request/identity frame from the client before re-transmitting the request:

```
Switch(config-if)# dot1x timeout tx-period 60
```

This example shows how to set 30 as the number of seconds that the switch ignores EAPOL packets from successfully authenticated clients:

```
Switch(config-if)# dot1x timeout ratelimit-period 30
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

**Related Commands**

Command	Description
<b>dot1x max-req</b>	Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.
<b>dot1x reauthentication</b>	Enables periodic re-authentication of the client.
<b>show dot1x</b>	Displays IEEE 802.1x status for all ports.

**dot1x violation-mode**

# dot1x violation-mode

Use the **dot1x violation-mode** interface configuration command to configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.

**dot1x violation-mode {shutdown | restrict | protect}**

**no dot1x violation-mode**

<b>Syntax Description</b>	<b>shutdown</b> Error disables the port or the virtual port on which a new unexpected MAC address occurs. <b>restrict</b> Generates a syslog error when a violation error occurs. <b>protect</b> Silently discards packets from any new MAC addresses. This is the default setting.
---------------------------	---

**Defaults** By default **dot1x violation-mode protect** is enabled.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(46)SE1	This command was introduced.

**Examples** This example shows how to configure an IEEE 802.1x-enabled port as error disabled and to shut down when a new device connects to the port:

```
Switch(config-if)# dot1x violation-mode shutdown
```

This example shows how to configure an IEEE 802.1x-enabled port to generate a system error message and change the port to restricted mode when a new device connects to the port:

```
Switch(config-if)# dot1x violation-mode restrict
```

This example shows how to configure an IEEE 802.1x-enabled port to ignore a new connected device when it is connected to the port:

```
Switch(config-if)# dot1x violation-mode protect
```

You can verify your settings by entering the **show dot1x [interface *interface-id*]** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.

# duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for a port. Use the **no** form of this command to return the port to its default value.

**duplex {auto | full | half}**

**no duplex**

Syntax Description	<b>auto</b> Enable automatic duplex configuration; port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
<b>full</b>	Enable full-duplex mode.
<b>half</b>	Enable half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s.

## Defaults

The default is **auto** for Fast Ethernet and Gigabit Ethernet ports.

The default is **half** for 100BASE-x (where -x is -BX, -FX, -FX-FE, or - LX) small form-factor pluggable (SFP) modules.

Duplex options are not supported on the 1000BASE-x (where -x is -BX, -CWDM, -LX, -SX, or -ZX) SFP modules.

For information about which SFP modules are supported on your switch, see the product release notes.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

For Fast Ethernet ports, setting the port to **auto** has the same effect as specifying **half** if the attached device does not autonegotiate the duplex parameter.

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.



### Note

Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do use the **auto** setting on the supported side.

**■ duplex**

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.

**Caution**

Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

**Examples**

This example shows how to configure an interface for full-duplex operation:

```
Switch(config-if)# duplex full
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show interfaces</a>	Displays the interface settings on the switch.
<a href="#">speed</a>	Sets the speed on a 10/100 or 10/100/1000 Mb/s interface.

# epm access-control open

Use the **epm access-control open** global configuration command on the switch stack or on a standalone switch to configure an open directive for ports that do not have an access control list (ACL) configured. Use the **no** form of this command to disable the open directive.

**epm access-control open**

**no epm access-control open**

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

**Defaults** The default directive applies.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

**Examples** This example shows how to configure an open directive.

```
Switch(config)# epm access-control open
```

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

Related Commands	Command	Description
	<b>show running-config</b>	Displays the operating configuration.

**errdisable detect cause**

# errdisable detect cause

To enable error-disable detection for a specific cause or for all causes, use the **errdisable detect cause** global configuration command. To disable the error-disable detection feature, use the **no** form of this command.

```
errdisable detect cause {all | bpduguard | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | link-flap | loopback | pagp-flap | psp | security-violation shutdown vlan | sfp-config-mismatch}
```

```
no errdisable detect cause {all | bpduguard | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | link-flap | loopback | pagp-flap | psp | security-violation shutdown vlan | sfp-config-mismatch}
```

For the bridge protocol data unit (BPDU) guard and port security, you can use this command to configure the switch to disable only a specific VLAN on a port instead of disabling the entire port.

When the per-VLAN error-disable feature is turned off and a BPDU guard violation occurs, the entire port is disabled. Use the **no** form of this command to disable the per-VLAN error-disable feature.

```
errdisable detect cause bpduguard shutdown vlan
```

```
no errdisable detect cause bpduguard shutdown vlan
```

Syntax Description	
<b>all</b>	Enable error detection for all error-disabled causes.
<b>bpduguard shutdown vlan</b>	Enable per-VLAN error-disable for BPDU guard.
<b>dhcp-rate-limit</b>	Enable error detection for DHCP snooping.
<b>dtp-flap</b>	Enable error detection for the Dynamic Trunking Protocol (DTP) flapping.
<b>gbic-invalid</b>	Enable error detection for an invalid Gigabit Interface Converter (GBIC) module.  <b>Note</b> This error refers to an invalid small form-factor pluggable (SFP) module on the switch.
<b>inline-power</b>	Enable error detection for inline power.
<b>link-flap</b>	Enable error detection for link-state flapping.
<b>loopback</b>	Enable error detection for detected loopbacks.
<b>pagp-flap</b>	Enable error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
<b>psp</b>	Enable error detection for protocol storm protection.
<b>security-violation</b>	Enable voice aware 802.1x security.
<b>shutdown vlan</b>	
<b>sfp-config-mismatch</b>	Enable error detection on an SFP configuration mismatch.

Command Default	Detection is enabled for all causes. All causes, except for per-VLAN error disabling, are configured to shut down the entire port.
-----------------	--

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

Command History	Release	Modification
	12.2(46)SE	The <b>security-violation shutdown vlan</b> keywords were added.
	12.2(58)SE	The <b>psp</b> keyword was introduced.

<b>Usage Guidelines</b>	A cause ( <b>link-flap</b> , <b>dhcp-rate-limit</b> , and so forth) is the reason why the error-disabled state occurred. When a cause is detected on a port, the port is placed in an error-disabled state, an operational state that is similar to a link-down state.
-------------------------	--

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU, voice aware 802.1x security, guard and port-security features, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command for the cause, the port is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually change the port from the error-disabled state.

For protocol storm protection, excess packets are dropped for a maximum of two virtual ports. Virtual port error disabling using the **psp** keyword is not supported for EtherChannel and Flexlink interfaces.

To verify your settings, enter the **show errdisable detect** privileged EXEC command.

<b>Examples</b>	This example shows how to enable error-disable detection for the link-flap error-disabled cause:
-----------------	--

```
Switch(config)# errdisable detect cause link-flap
```

This command shows how to globally configure BPDU guard for per-VLAN error disable:

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

This command shows how to globally configure voice aware 802.1x security for per-VLAN error disable:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

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

<b>Related Commands</b>	
-------------------------	--

Command	Description
<a href="#">show errdisable detect</a>	Displays error-disabled detection information.
<a href="#">show interfaces status err-disabled</a>	Displays interface status or a list of interfaces in the error-disabled state.
<a href="#">clear errdisable interface</a>	Clears the error-disabled state from a port or VLAN that was error disabled by the per-VLAN error disable feature.

**errdisable detect cause small-frame**

# errdisable detect cause small-frame

Use the **errdisable detect cause small-frame** global configuration command to allow any switch port to be error disabled if incoming VLAN-tagged packets are small frames (67 bytes or less) and arrive at the minimum configured rate (the threshold). Use the **no** form of this command to return to the default setting.

**errdisable detect cause small-frame**

**no errdisable detect cause small-frame**

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

**Defaults** This feature is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(44)SE	This command was introduced.

**Usage Guidelines** This command globally enables the small-frame arrival feature. Use the **small violation-rate** interface configuration command to set the threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** global configuration command.

**Examples** This example shows how to enable the switch ports to be put into the error-disabled mode if incoming small frames arrive at the configured threshold:

```
Switch(config)# errdisable detect cause small-frame
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Related Commands	Command	Description
	<b>errdisable recovery cause small-frame</b>	Enables the recovery timer.
	<b>errdisable recovery interval <i>interval</i></b>	Specifies the time to recover from the specified error-disabled state.
	<b>show interfaces</b>	Displays the interface settings on the switch, including input and output flow control.
	<b>small violation-rate</b>	Configures the rate (threshold) for incoming small frames to cause a port to be put into the error-disabled state.

---

 errdisable recovery cause small-frame

# errdisable recovery cause small-frame

Use the **errdisable recovery cause small-frame** global configuration command on the switch to enable the recovery timer for ports to be automatically re-enabled after they are error disabled by the arrival of small frames. Use the **no** form of this command to return to the default setting.

**errdisable recovery cause small-frame**

**no errdisable recovery cause small-frame**

---

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

---

**Defaults** This feature is disabled.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(44)SE	This command was introduced.

---

**Usage Guidelines** This command enables the recovery timer for error-disabled ports. You configure the recovery time by using the errdisable **recovery interval *interval*** interface configuration command.

---

**Examples** This example shows how to set the recovery timer:

```
Switch(config)# errdisable recovery cause small-frame
```

You can verify your setting by entering the **show interfaces** user EXEC command.

---

Related Commands	Command	Description
	<b>errdisable detect cause small-frame</b>	Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the configured minimum size and arrives at the specified rate (threshold).
	<b>show interfaces</b>	Displays the interface settings on the switch, including input and output flow control.
	<b>small violation-rate</b>	Configures the size for an incoming (small) frame to cause a port to be put into the error-disabled state.

---

# errdisable recovery

Use the **errdisable recovery** global configuration command to configure the recover mechanism variables. Use the **no** form of this command to return to the default setting.

```
errdisable recovery {cause {all | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | link-flap | loopback | pagp-flap | psecure-violation | psp |
security-violation | sfp-mismatch | storm-control | udld | vmps} | {interval interval}}
```

```
no errdisable recovery {cause {all | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | link-flap | loopback | pagp-flap | psecure-violation | psp |
security-violation | sfp-mismatch | storm-control | udld | vmps} | {interval interval}}
```

Syntax Description	
<b>cause</b>	Enable the error-disabled mechanism to recover from a specific cause.
<b>all</b>	Enable the timer to recover from all error-disabled causes.
<b>bpdukguard</b>	Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
<b>channel-misconfig</b>	Enable the timer to recover from the EtherChannel misconfiguration error-disabled state.
<b>dhcp-rate-limit</b>	Enable the timer to recover from the DHCP snooping error-disabled state.
<b>dtp-flap</b>	Enable the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.
<b>gbic-invalid</b>	Enable the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state. <b>Note</b> This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
<b>inline-power</b>	Enable error detection for inline-power.
<b>link-flap</b>	Enable the timer to recover from the link-flap error-disabled state.
<b>loopback</b>	Enable the timer to recover from a loopback error-disabled state.
<b>pagp-flap</b>	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
<b>psp</b>	Enable the timer to recover from the protocol storm protection error-disabled state.
<b>psecure-violation</b>	Enable the timer to recover from a port security violation disable state.
<b>security-violation</b>	Enable the timer to recover from an IEEE 802.1x-violation disabled state.
<b>sfp-mismatch</b>	Enable error detection on an SFP configuration mismatch.
<b>storm-control</b>	Enable the timer to recover from the storm-control error-disabled state.
<b>udld</b>	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.

**errdisable recovery**


---

<b>vmps</b>	Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.
<b>interval interval</b>	Specify the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.
<b>Note</b>	The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

---

**Defaults**

Recovery is disabled for all causes.

The default recovery interval is 300 seconds.

**Command Modes**

Global configuration

**Command History**


---

<b>Release</b>	<b>Modification</b>
12.2(37)SE	The per-VLAN error-detection feature was added. The <b>inline-power</b> and <b>sfp-mismatch</b> keywords were added.
12.2(58)SE	The <b>psp</b> keyword was introduced.

---

**Usage Guidelines**

A cause (**link-flap**, **bpduguard**, and so forth) is defined as the reason that the error-disabled state occurred. When a cause is detected on a port, the port is placed in the error-disabled state, an operational state similar to the link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you do not enable the recovery for the cause, the port stays in the error-disabled state until you enter the **shutdown** and the **no shutdown** interface configuration commands. If you enable the recovery for a cause, the port is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** and then the **no shutdown** commands to manually recover a port from the error-disabled state.

**Examples**

This example shows how to enable the recovery timer for the BPDU guard error-disabled cause:

```
Switch(config)# errdisable recovery cause bpduguard
```

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

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

Related Commands	Command	Description
	<a href="#">show errdisable recovery</a>	Displays error-disabled recovery timer information.
	<a href="#">show interfaces status err-disabled</a>	Displays interface status or a list of interfaces in error-disabled state.
	<a href="#">clear errdisable interface</a>	Clears the error-disabled state from a port or VLAN that was error disabled by the per-VLAN error disable feature.

**exception crashinfo**

# exception crashinfo

Use the **exception crashinfo** global configuration command to configure the switch to create the extended crashinfo file when the Cisco IOS image fails. Use the **no** form of this command to disable this feature.

**exception crashinfo**

**no exception crashinfo**

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

**Defaults** The switch creates the extended crashinfo file.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

The basic crashinfo file includes the Cisco IOS name and version that failed a list of the processor registers. The extended crashinfo file includes additional information that can help determine the cause of the switch failure.

Use the **no exception crashinfo** global configuration command to configure the switch to not create the extended crashinfo file.

---

### Examples

This example shows how to configure the switch to not create the extended crashinfo file:

```
Switch(config)# no exception crashinfo
```

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

---

### Related Commands

Command	Description
<b>show running-config</b>	Displays the operating configuration, including defined macros.

# fallback profile

Use the **fallback profile** global configuration command to create a fallback profile for web authentication. To return to the default setting, use the **no** form of this command.

**fallback profile** *profile*

**no fallback profile**

<b>Syntax Description</b>	<i>profile</i>	Specify the fallback profile for clients that do not support IEEE 802.1x authentication.
<b>Defaults</b>	No fallback profile is configured.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(35)SE	This command was introduced.
<b>Usage Guidelines</b>	<p>The fallback profile is used to define the IEEE 802.1x fallback behavior for IEEE 802.1x ports that do not have supplicants. The only supported behavior is to fall back to web authentication.</p> <p>After entering the <b>fallback profile</b> command, you enter profile configuration mode, and these configuration commands are available:</p> <ul style="list-style-type: none"> <li>• <b>ip</b>: Create an IP configuration.</li> <li>• <b>access-group</b>: Specify access control for packets sent by hosts that have not yet been authenticated.</li> <li>• <b>admission</b>: Apply an IP admission rule.</li> </ul>	
<b>Examples</b>	<p>This example shows how to create a fallback profile to be used with web authentication:</p> <pre>Switch# configure terminal Switch(config)# ip admission name rule1 proxy http Switch(config)# fallback profile profile1 Switch(config-fallback-profile)# ip access-group default-policy in Switch(config-fallback-profile)# ip admission rule1 Switch(config-fallback-profile)# exit Switch(config-if)# dot1x fallback profile1 Switch(config-if)# end</pre>	

You can verify your settings by entering the **show running-configuration [interface *interface-id*]** privileged EXEC command.

**■ fallback profile**

Related Commands	Command	Description
	<b>dot1x fallback</b>	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<b>ip admission</b>	Enable web authentication on a switch port
	<b>ip admission name proxy http</b>	Enable web authentication globally on a switch
	<b>show dot1x [interface <i>interface-id</i>]</b>	Displays IEEE 802.1x status for the specified port.
	<b>show fallback profile</b>	Display the configured profiles on a switch.

# flowcontrol

Use the **flowcontrol** interface configuration command to set the receive flow-control state for an interface. When flow control **send** is operable and on for a device and it detects any congestion at its end, it notifies the link partner or the remote device of the congestion by sending a pause frame. When flow control **receive** is on for a device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period.

Use the **receive off** keywords to disable flow control.

**flowcontrol receive {desired | off | on}**



The switch can receive, but not send, pause frames.

## Syntax Description

<b>receive</b>	Set whether the interface can receive flow-control packets from a remote device.
<b>desired</b>	Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.
<b>off</b>	Turn off the ability of an attached device to send flow-control packets to an interface.
<b>on</b>	Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

## Defaults

The default is **flowcontrol receive off**.

## Command Modes

Interface configuration

## Command History

## Usage Guidelines

The switch does not support sending flow-control pause frames.

Note that the **on** and **desired** keywords have the same result.

When you use the **flowcontrol** command to set a port to control traffic rates during congestion, you are setting flow control on a port to one of these conditions:

- **receive on** or **desired**: The port cannot send pause frames, but can operate with an attached device that is required to or is able to send pause frames. The port can receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

**■ flowcontrol**

[Table 2-13](#) shows the flow control results on local and remote ports for a combination of settings. The table assumes that **receive desired** has the same results as using the **receive on** keywords.

**Table 1-13 Flow Control Settings and Local and Remote Port Flow Control Resolution**

<b>Flow Control Settings</b>		<b>Flow Control Resolution</b>	
<b>Local Device</b>	<b>Remote Device</b>	<b>Local Device</b>	<b>Remote Device</b>
<b>send off/receive on</b>	<b>send on/receive on</b>	Receives only	Sends and receives
	<b>send on/receive off</b>	Receives only	Sends only
	<b>send desired/receive on</b>	Receives only	Sends and receives
	<b>send desired/receive off</b>	Receives only	Sends only
	<b>send off/receive on</b>	Receives only	Receives only
	<b>send off/receive off</b>	Does not send or receive	Does not send or receive
<b>send off/receive off</b>	<b>send on/receive on</b>	Does not send or receive	Does not send or receive
	<b>send on/receive off</b>	Does not send or receive	Does not send or receive
	<b>send desired/receive on</b>	Does not send or receive	Does not send or receive
	<b>send desired/receive off</b>	Does not send or receive	Does not send or receive
	<b>send off/receive on</b>	Does not send or receive	Does not send or receive
	<b>send off/receive off</b>	Does not send or receive	Does not send or receive

**Examples**

This example shows how to configure the local port to not support flow control by the remote port:

```
Switch(config-if)# flowcontrol receive off
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show interfaces</b>	Displays the interface settings on the switch, including input and output flow control.

# interface port-channel

Use the **interface port-channel** global configuration command to access or create the port-channel logical interface. Use the **no** form of this command to remove the port-channel.

**interface port-channel** *port-channel-number*

**no interface port-channel** *port-channel-number*

---

## Syntax Description

*port-channel-number* Port-channel number. The range is 1 to .

---

## Defaults

No port-channel logical interfaces are defined.

---

## Command Modes

Global configuration

---

## Command History

### Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Only one port channel in a channel group is allowed.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the physical port and not on the port-channel interface.
- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

---

## Examples

This example shows how to create a port-channel interface with a port channel number of 5:

```
Switch(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

---

## Related Commands

**■ interface port-channel**

Command	Description
<b>channel-group</b>	Assigns an Ethernet port to an EtherChannel group.
<b>show etherchannel</b>	Displays EtherChannel information for a channel.
<b>show running-config</b>	Displays the current operating configuration.

# interface range

Use the **interface range** global configuration command to enter interface range configuration mode and to execute a command on multiple ports at the same time. Use the **no** form of this command to remove an interface range.

**interface range {port-range | macro name}**

**no interface range {port-range | macro name}**

<b>Syntax Description</b>	<p><b>port-range</b> Port range. For a list of valid values for <i>port-range</i>, see the “Usage Guidelines” section.</p> <p><b>macro name</b> Specify the name of a macro.</p>
---------------------------	--

**Defaults** This command has no default setting.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

When you enter interface range configuration mode, all interface parameters you enter are attributed to all interfaces within the range.

For VLANs, you can use the **interface range** command only on existing VLAN switch virtual interfaces (SVIs). To display VLAN SVIs, enter the **show running-config** privileged EXEC command. VLANs not displayed cannot be used in the **interface range** command. The commands entered under **interface range** command are applied to all existing VLAN SVIs in the range.

All configuration changes made to an interface range are saved to NVRAM, but the interface range itself is not saved to NVRAM.

You can enter the interface range in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined interface-range macro

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs. However, you can define up to five interface ranges with a single command, with each range separated by a comma.

**■ interface range**

Valid values for *port-range* type and interface:

- **vlan** *vlan-ID*, where VLAN ID is from 1 to 4094
- **fastethernet** *module/{first port}* - *{last port}*, where module is always **0**
- **gigabitethernet** *module/{first port}* - *{last port}*, where module is always **0**

For physical interfaces:

- module is always 0
- **port-channel** *port-channel-number* - *port-channel-number*, where *port-channel-number* is from 1 to



**Note** When you use the **interface range** command with port channels, the first and last port channel number in the range must be active port channels.

When you define a range, you must enter a space between the first entry and the hyphen (-):

When you define multiple ranges, you must still enter a space after the first entry and before the comma (,):

You cannot specify both a macro and an interface range in the same command.

You can also specify a single interface in *port-range*. The command is then similar to the **interface interface-id** global configuration command.

For more information about configuring interface ranges, see the software configuration guide for this release.

**Examples**

This example shows how to use the **interface range** command to enter interface-range configuration mode to apply commands to two ports:

This example shows how to use a port-range macro *macro1* for the same function. The advantage is that you can reuse *macro1* until you delete it.

```
Switch(config)# interface range macro macro1
Switch(config-if-range) #
```

**Related Commands**

Command	Description
<b>define interface-range</b>	Creates an interface range macro.
<b>show running-config</b>	Displays the configuration information currently running on the switch.

# interface vlan

Use the **interface vlan** global configuration command to create or access a and to enter interface configuration mode. Use the **no** form of this command to delete .

**interface vlan *vlan-id***

**no interface vlan *vlan-id***

<b>Syntax Description</b>	<i>vlan-id</i> VLAN number. The range is 1 to 4094.
<b>Defaults</b>	The default VLAN interface is VLAN 1.
<b>Command Modes</b>	Global configuration
<b>Command History</b>	
<b>Usage Guidelines</b>	<p>are created the first time that you enter the <b>interface vlan <i>vlan-id</i></b> command for a particular VLAN. The <i>vlan-id</i> corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.</p> <p>If you delete by entering the <b>no interface vlan <i>vlan-id</i></b> command, the deleted interface is no longer visible in the output from the <b>show interfaces</b> privileged EXEC command.</p>
 <b>Note</b>	You cannot delete the VLAN 1 interface.
	You can re-instate a deleted by entering the <b>interface vlan <i>vlan-id</i></b> command for the deleted interface. The interface comes back up, but the previous configuration is gone.

**■ interface vlan****Examples**

This example shows how to create a new VLAN with VLAN ID 23 and to enter interface configuration mode:

```
Switch(config)# interface vlan 23
Switch(config-if)#

```

You can verify your setting by entering the [show interfaces](#) and [show interfaces vlan \*vlan-id\*](#) privileged EXEC commands.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show interfaces vlan <i>vlan-id</i></a>	Displays the administrative and operational status of all interfaces or the specified VLAN.

# ip access-group

Use the **ip access-group** interface configuration command to control access to a Layer 2 or Layer 3 interface. Use the **no** form of this command to remove all access groups or the specified access group from the interface.

**ip access-group {access-list-number | name} {in | out}**

**no ip access-group [access-list-number | name] {in | out}**

Syntax Description		
	<i>access-list-number</i>	The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699.
	<i>name</i>	The name of an IP ACL, specified in the <b>ip access-list</b> global configuration command.
	<b>in</b>	Specify filtering on inbound packets.
	<b>out</b>	Specify filtering on outbound packets. This keyword is valid only on interfaces.

**Defaults** No access list is applied to the interface.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

You can apply named or numbered standard or extended IP access lists to an interface. To define an access list by name, use the **ip access-list** global configuration command. To define a numbered access list, use the **access list** global configuration command. You can use numbered standard access lists ranging from 1 to 99 and 1300 to 1999 or extended access lists ranging from 100 to 199 and 2000 to 2699.

You can use this command to apply an access list to a Layer 2 or Layer 3 interface. However, note these limitations:

- You can apply an ACL to Layer 2 ports in the inbound direction only.
- You can apply only one IP ACL and one MAC ACL per interface.
- do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to an interface only filters IP packets. To filter non-IP packets, use the **mac access-group** interface configuration command with MAC extended ACLs.
- When an input router ACL and input port ACLs exist in an switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.

**ip access-group**

You can apply IP ACLs to both outbound or inbound Layer 3 interfaces.

A Layer 3 interface can have one IP ACL applied in each direction.

For standard inbound access lists, after the switch receives a packet, it checks the source address of the packet against the access list. IP extended access lists can optionally check other fields in the packet, such as the destination IP address, protocol type, or port numbers. If the access list permits the packet, the switch continues to process the packet. If the access list denies the packet, the switch discards the packet.

If the specified access list does not exist, all packets are passed.

**Examples**

This example shows how to apply IP access list 101 to inbound packets on a port:

```
Switch(config-if)# ip access-group 101 in
```

You can verify your settings by entering the **show ip interface**, **show access-lists**, or **show ip access-lists** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>access list</b>	Configures a numbered ACL.
<b>ip access-list</b>	Configures a named ACL.
<b>show access-lists</b>	Displays ACLs configured on the switch.
<b>show ip access-lists</b>	Displays IP ACLs configured on the switch.
<b>show ip interface</b>	Displays information about interface status and configuration.

# ip address

Use the **ip address** interface configuration command to set an IP address for the Layer 2 switch. Use the **no** form of this command to remove an IP address or to disable IP processing.

**ip address ip-address subnet-mask [secondary]**

**no ip address [ip-address subnet-mask] [secondary]**

## Syntax Description

<i>ip-address</i>	IP address.
<i>subnet-mask</i>	Mask for the associated IP subnet.
<b>secondary</b>	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

## Defaults

No IP address is defined.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch will be lost. Hosts can find subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the switch detects another host using one of its IP addresses, it will send an error message to the console.

You can use the optional keyword **secondary** to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.



**Note** If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or the DHCP server cannot reassign the address.

## Examples

This example shows how to configure the IP address for the Layer 2 switch on a subnetted network:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

**■ ip address**

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

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the running configuration on the switch.

# ip admission

Use the **ip admission** interface configuration command to enable web authentication. You can also use this command in fallback-profile mode. Use the **no** form of this command to disable web authentication.

**ip admission rule**

**no ip admission**

<b>Syntax Description</b>	<b>rule</b> Apply an IP admission rule to the interface.												
<b>Command Modes</b>	Global configuration												
<b>Command History</b>	<table border="1"> <thead> <tr> <th><b>Release</b></th><th><b>Modification</b></th></tr> </thead> <tbody> <tr> <td>12.2(35)SE</td><td>This command was introduced.</td></tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	12.2(35)SE	This command was introduced.								
<b>Release</b>	<b>Modification</b>												
12.2(35)SE	This command was introduced.												
<b>Usage Guidelines</b>	The <b>ip admission</b> command applies a web authentication rule to a switch port.												
<b>Examples</b>	<p>This example shows how to apply a web authentication rule to a switchport:</p> <pre>Switch# configure terminal Switch(config-if)# ip admission rule1</pre> <p>This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.</p> <pre>Switch# configure terminal Switch(config)# fallback profile profile1 Switch(config)# ip admission name rule1 Switch(config)# end</pre>												
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><a href="#">dot1x fallback</a></td><td>Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.</td></tr> <tr> <td><a href="#">fallback profile</a></td><td>Enable web authentication on a port</td></tr> <tr> <td><a href="#">ip admission name</a></td><td>Enable web authentication globally on a switch</td></tr> <tr> <td><a href="#">proxy http</a></td><td></td></tr> <tr> <td><a href="#">show ip admission</a></td><td>Displays information about NAC cached entries or the NAC configuration. For more information, see the <i>Network Admission Control Software Configuration Guide</i> on Cisco.com.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">dot1x fallback</a>	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.	<a href="#">fallback profile</a>	Enable web authentication on a port	<a href="#">ip admission name</a>	Enable web authentication globally on a switch	<a href="#">proxy http</a>		<a href="#">show ip admission</a>	Displays information about NAC cached entries or the NAC configuration. For more information, see the <i>Network Admission Control Software Configuration Guide</i> on Cisco.com.
<b>Command</b>	<b>Description</b>												
<a href="#">dot1x fallback</a>	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.												
<a href="#">fallback profile</a>	Enable web authentication on a port												
<a href="#">ip admission name</a>	Enable web authentication globally on a switch												
<a href="#">proxy http</a>													
<a href="#">show ip admission</a>	Displays information about NAC cached entries or the NAC configuration. For more information, see the <i>Network Admission Control Software Configuration Guide</i> on Cisco.com.												

---

■ ip admission name proxy http

# ip admission name proxy http

Use the **ip admission name proxy http** global configuration command to enable web authentication.  
Use the **no** form of this command to disable web authentication.

**ip admission name proxy http**

**no ip admission name proxy http**

---

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

---

**Defaults** Web authentication is disabled.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.2(35)SE	This command was introduced.

---



---

**Usage Guidelines** The **ip admission name proxy http** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

---

**Examples** This example shows how to configure only web authentication on a switchport:

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switchport.

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

---

**Related Commands**

Command	Description
<b>dot1x fallback</b>	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<b>fallback profile</b>	Create a web authentication fallback profile.
<b>ip admission</b>	Enable web authentication on a port
<b>show ip admission</b>	Displays information about NAC cached entries or the NAC configuration. For more information, see the <i>Network Admission Control Software Configuration Guide</i> on Cisco.com.

**ip arp inspection filter vlan**

# ip arp inspection filter vlan

Use the **ip arp inspection filter vlan** global configuration command to permit or deny Address Resolution Protocol (ARP) requests and responses from a host configured with a static IP address when dynamic ARP inspection is enabled. Use the **no** form of this command to return to the default settings.

**ip arp inspection filter *arp-acl-name* *vlan* *vlan-range* [static]**

**no ip arp inspection filter *arp-acl-name* *vlan* *vlan-range* [static]**

<b>Syntax Description</b>	<table border="0"> <tr> <td><i>arp-acl-name</i></td><td>ARP access control list (ACL) name.</td></tr> <tr> <td><i>vlan-range</i></td><td>VLAN number or range.</td></tr> <tr> <td></td><td>You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td></tr> <tr> <td><b>static</b></td><td>(Optional) Specify <b>static</b> to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used.  If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.</td></tr> </table>	<i>arp-acl-name</i>	ARP access control list (ACL) name.	<i>vlan-range</i>	VLAN number or range.		You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.	<b>static</b>	(Optional) Specify <b>static</b> to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used.  If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.
<i>arp-acl-name</i>	ARP access control list (ACL) name.								
<i>vlan-range</i>	VLAN number or range.								
	You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.								
<b>static</b>	(Optional) Specify <b>static</b> to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used.  If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL.								

**Defaults** No defined ARP ACLs are applied to any VLAN.

**Command Modes** Global configuration

**Command History**

**Usage Guidelines** When an ARP ACL is applied to a VLAN for dynamic ARP inspection, only the ARP packets with IP-to-MAC address bindings are compared against the ACL. If the ACL permits a packet, the switch forwards it. All other packet types are bridged in the ingress VLAN without validation.

If the switch denies a packet because of an explicit deny statement in the ACL, the packet is dropped. If the switch denies a packet because of an implicit deny statement, the packet is then compared against the list of DHCP bindings (unless the ACL is *static*, which means that packets are not compared against the bindings).

Use the **arp access-list *acl-name*** global configuration command to define the ARP ACL or to add clauses to the end of a predefined list.

**Examples**

This example shows how to apply the ARP ACL *static-hosts* to VLAN 1 for dynamic ARP inspection:

```
Switch(config)# ip arp inspection filter static-hosts vlan 1
```

You can verify your settings by entering the **show ip arp inspection vlan 1** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP ACL.
<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the DHCP bindings.
<a href="#">permit (ARP access-list configuration)</a>	Permits an ARP packet based on matches against the DHCP bindings.
<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.
<a href="#">show inventory vlan <i>vlan-range</i></a>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

**ip arp inspection limit**

# ip arp inspection limit

Use the **ip arp inspection limit** interface configuration command to limit the rate of incoming Address Resolution Protocol (ARP) requests and responses on an interface. It prevents dynamic ARP inspection from using all of the switch resources if a denial-of-service attack occurs. Use the **no** form of this command to return to the default settings.

**ip arp inspection limit {rate pps [burst interval seconds] | none}**

**no ip arp inspection limit**

<b>Syntax Description</b>	<b>rate pps</b> Specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 packets per second (pps). <b>burst interval seconds</b> (Optional) Specify the consecutive interval in seconds, over which the interface is monitored for a high rate of ARP packets. The range is 1 to 15 seconds. <b>none</b> Specify no upper limit for the rate of incoming ARP packets that can be processed.
---------------------------	---

**Defaults**

The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second.

The rate is unlimited on all trusted interfaces.

The burst interval is 1 second.

**Command Modes**

Interface configuration

**Command History****Usage Guidelines**

The rate applies to both trusted and untrusted interfaces. Configure appropriate rates on trunks to process packets across multiple dynamic ARP inspection-enabled VLANs, or use the **none** keyword to make the rate unlimited.

After a switch receives more than the configured rate of packets every second consecutively over a number of burst seconds, the interface is placed into an error-disabled state.

Unless you explicitly configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the **no ip arp inspection limit** interface configuration command, the interface reverts to its default rate limit.

You should configure trunk ports with higher rates to reflect their aggregation. When the rate of incoming packets exceeds the user-configured rate, the switch places the interface into an error-disabled state. The error-disabled recovery feature automatically removes the port from the error-disabled state according to the recovery setting.

The rate of incoming ARP packets on EtherChannel ports equals the sum of the incoming rate of ARP packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on all the channel members.

---

**Examples**

This example shows how to limit the rate of incoming ARP requests on a port to 25 pps and to set the interface monitoring interval to 5 consecutive seconds:

```
Switch(config-if)# ip arp inspection limit rate 25 burst interval 5
```

You can verify your settings by entering the **show ip arp inspection interfaces *interface-id*** privileged EXEC command.

---

**Related Commands**

Command	Description
<b>show inventory interfaces</b>	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.

---

**ip arp inspection log-buffer**

# ip arp inspection log-buffer

Use the **ip arp inspection log-buffer** global configuration command to configure the dynamic Address Resolution Protocol (ARP) inspection logging buffer. Use the **no** form of this command to return to the default settings.

**ip arp inspection log-buffer {entries number | logs number interval seconds}**

**no ip arp inspection log-buffer {entries | logs}**

<b>Syntax Description</b>	
<b>entries number</b>	Number of entries to be logged in the buffer. The range is 0 to 1024.
<b>logs number</b>	Number of entries needed in the specified interval to generate system messages.
<b>interval seconds</b>	For <b>logs number</b> , the range is 0 to 1024. A 0 value means that the entry is placed in the log buffer, but a system message is not generated. For <b>interval seconds</b> , the range is 0 to 86400 seconds (1 day). A 0 value means that a system message is immediately generated (and the log buffer is always empty).

**Defaults**

When dynamic ARP inspection is enabled, denied or dropped ARP packets are logged.

The number of log entries is 32.

The number of system messages is limited to 5 per second.

The logging-rate interval is 1 second.

**Command Modes**

Global configuration

**Command History****Usage Guidelines**

A value of 0 is not allowed for both the **logs** and the **interval** keywords.

The **logs** and **interval** settings interact. If the **logs number X** is greater than **interval seconds Y**, X divided by Y (X/Y) system messages are sent every second. Otherwise, one system message is sent every Y divided by X (Y/X) seconds. For example, if the **logs number** is 20 and the **interval seconds** is 4, the switch generates system messages for five entries every second while there are entries in the log buffer.

A log buffer entry can represent more than one packet. For example, if an interface receives many packets on the same VLAN with the same ARP parameters, the switch combines the packets as one entry in the log buffer and generates a system message as a single entry.

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the output display for the **show ip arp inspection log** privileged EXEC command is affected. A -- in the output display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer, or increase the logging rate.

**Examples**

This example shows how to configure the logging buffer to hold up to 45 entries:

```
Switch(config)# ip arp inspection log-buffer entries 45
```

This example shows how to configure the logging rate to 20 log entries per 4 seconds. With this configuration, the switch generates system messages for five entries every second while there are entries in the log buffer.

```
Switch(config)# ip arp inspection log-buffer logs 20 interval 4
```

You can verify your settings by entering the **show ip arp inspection log** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
<a href="#">clear ip arp inspection log</a>	Clears the dynamic ARP inspection log buffer.
<a href="#">ip arp inspection vlan logging</a>	Controls the type of packets that are logged per VLAN.
<a href="#">show inventory log</a>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

**ip arp inspection trust**

Use the **ip arp inspection trust** interface configuration command to configure an interface trust state that determines which incoming Address Resolution Protocol (ARP) packets are inspected. Use the **no** form of this command to return to the default setting.

**ip arp inspection trust**

**no ip arp inspection trust**

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

**Defaults** The interface is untrusted.

**Command Modes** Interface configuration

**Command History**

**Usage Guidelines** The switch does not check ARP packets that it receives on the trusted interface; it simply forwards the packets.

For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command.

**Examples** This example shows how to configure a port to be trusted:

```
Switch(config-if)# ip arp inspection trust
```

You can verify your setting by entering the **show ip arp inspection interfaces interface-id** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.
	<a href="#">show inventory interfaces</a>	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
	<a href="#">show inventory log</a>	Displays the configuration and contents of the dynamic ARP inspection log buffer.

**ip arp inspection validate**

# ip arp inspection validate

Use the **ip arp inspection validate** global configuration command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to return to the default settings.

**ip arp inspection validate {[src-mac] [dst-mac] [ip [allow zeros]]}**

**no ip arp inspection validate [src-mac] [dst-mac] [ip [allow zeros]]**

Syntax Description		
	<b>src-mac</b>	Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.  When enabled, packets with different MAC addresses are classified as invalid and are dropped.
	<b>dst-mac</b>	Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses.  When enabled, packets with different MAC addresses are classified as invalid and are dropped.
	<b>ip</b>	Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.  Sender IP addresses are compared in all ARP requests and responses. Target IP addresses are checked only in ARP responses.
	<b>allow-zeros</b>	Modifies the IP validation test so that ARPs with a sender address of 0.0.0.0 (ARP probes) are not denied.

**Defaults** No checks are performed.

**Command Modes** Global configuration

**Command History**

**Usage Guidelines**

You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables **src-mac** and **dst-mac** validations, and a second command enables IP validation only, the **src-mac** and **dst-mac** validations are disabled as a result of the second command.

The **allow-zeros** keyword interacts with ARP access control lists (ACLs) in this way:

- If you configure an ARP ACL to deny ARP probes, they are dropped even if the **allow-zero** keyword is specified.
- If you configure an ARP ACL that specifically permits ARP probes and configure the **ip arp inspection validate ip** command, ARP probes are dropped unless you enter the **allow-zeros** keyword.

The **no** form of the command disables only the specified checks. If none of the options are enabled, all checks are disabled.

**Examples**

This example shows how to enable source MAC validation:

```
Switch(config)# ip arp inspection validate src-mac
```

You can verify your setting by entering the **show ip arp inspection vlan *vlan-range*** privileged EXEC command.

**Related Commands**

Command	Description
<b>show inventory vlan <i>vlan-range</i></b>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

**ip arp inspection vlan**

Use the **ip arp inspection vlan** global configuration command to enable dynamic Address Resolution Protocol (ARP) inspection on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**ip arp inspection vlan *vlan-range***

**no ip arp inspection vlan *vlan-range***

<b>Syntax Description</b>	<i>vlan-range</i>	VLAN number or range.  You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>Defaults</b>		ARP inspection is disabled on all VLANs.
<b>Command Modes</b>		Global configuration
<b>Command History</b>		
<b>Usage Guidelines</b>		You must specify the VLANs on which to enable dynamic ARP inspection.  Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, or private VLAN ports.
<b>Examples</b>		This example shows how to enable dynamic ARP inspection on VLAN 1:  Switch(config)# <b>ip arp inspection vlan 1</b>
		You can verify your setting by entering the <b>show ip arp inspection vlan <i>vlan-range</i></b> privileged EXEC command.
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>arp access-list</b>	Defines an ARP access control list (ACL).
	<b>show inventory vlan <i>vlan-range</i></b>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

# ip arp inspection vlan logging

Use the **ip arp inspection vlan logging** global configuration command to control the type of packets that are logged per VLAN. Use the **no** form of this command to disable this logging control.

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit} | arp-probe}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings | arp-probe}
```

Syntax Description	
	<p><i>vlan-range</i> Specify the VLANs configured for logging. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</p>
<b>acl-match {matchlog   none}</b>	<p>Specify that the logging of packets is based on access control list (ACL) matches. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>matchlog</b>—Log packets based on the logging configuration specified in the access control entries (ACE). If you specify the <b>matchlog</b> keyword in this command and the <b>log</b> keyword in the <b>permit</b> or <b>deny</b> ARP access-list configuration command, Address Resolution Protocol (ARP) packets permitted or denied by the ACL are logged.</li> <li>• <b>none</b>—Do not log packets that match ACLs.</li> </ul>
<b>dhcp-bindings {permit   all   none}</b>	<p>Specify the logging of packets is based on Dynamic Host Configuration Protocol (DHCP) binding matches. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Log all packets that match DHCP bindings.</li> <li>• <b>none</b>—Do not log packets that match DHCP bindings.</li> <li>• <b>permit</b>—Log DHCP-binding permitted packets.</li> </ul>
<b>arp-probe</b>	Specify logging of packets permitted specifically because they are ARP probes.

**Defaults** All denied or all dropped packets are logged. ARP probe packets are not logged.

**Command Modes** Global configuration

## Command History

**ip arp inspection vlan logging****Usage Guidelines**

The term *logged* means that the entry is placed into the log buffer and that a system message is generated.

The **acl-match** and **dhcp-bindings** keywords merge with each other; that is, when you configure an ACL match, the DHCP bindings configuration is not disabled. Use the **no** form of the command to reset the logging criteria to their defaults. If neither option is specified, all types of logging are reset to log when ARP packets are denied. These are the options:

- **acl-match**—Logging on ACL matches is reset to log on deny.
- **dhcp-bindings**—Logging on DHCP binding matches is reset to log on deny.

If neither the **acl-match** or the **dhcp-bindings** keywords are specified, all denied packets are logged.

The implicit deny at the end of an ACL does not include the **log** keyword. This means that when you use the **static** keyword in the **ip arp inspection filter vlan** global configuration command, the ACL overrides the DHCP bindings. Some denied packets might not be logged unless you explicitly specify the **deny ip any mac any log** ACE at the end of the ARP ACL.

**Examples**

This example shows how to configure ARP inspection on VLAN 1 to log packets that match the **permit** commands in the ACL:

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

You can verify your settings by entering the **show ip arp inspection vlan *vlan-range*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">arp access-list</a>	Defines an ARP ACL.
<a href="#">clear ip arp inspection log</a>	Clears the dynamic ARP inspection log buffer.
<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.
<a href="#">show inventory log</a>	Displays the configuration and contents of the dynamic ARP inspection log buffer.
<a href="#">show inventory vlan <i>vlan-range</i></a>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

# ip device tracking probe

Use the **ip device tracking probe** global configuration command to configure the IP device tracking table for Address Resolution Protocol (ARP) probes. Use the **no** form of this command to disable ARP probes.

**ip device tracking probe {count | interval | use-svi}**

**no ip device tracking probe {count | interval | use-svi}**

<b>Syntax Description</b>	<b>count number</b> Sets the number of times that the switch sends the ARP probe. The range is from 1 to 255. <b>interval seconds</b> Sets the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds. <b>use-svi</b> Uses the switch virtual interface (SVI) IP address as source of ARP probes.
---------------------------	---

<b>Command Default</b>	The count number is 3. The interval is 30 seconds. The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.
------------------------	--

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(55)SE	The <b>use-svi</b> keyword was added.

<b>Usage Guidelines</b>	Use the <b>count</b> keyword option to set the number of times that the switch sends the ARP probe. The range is from 1 to 255. Use the <b>interval</b> keyword option to set the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds. Use the <b>use-svi</b> keyword option to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source ip address 0.0.0.0 for switch ports is used and the ARP probes drop. Use the <b>show ip device tracking all</b> command to display information about entries in the IP device tracking table. For more information about this command, see the Cisco IOS Security Command Reference, Release 12.4T.
-------------------------	--

<b>Examples</b>	This example shows how to set SVI as the source for ARP probes:
	<pre>Switch(config)# ip device tracking probe use-svi Switch(config)# </pre>

■ ip device tracking probe

Related Commands	Command	Description
	<b>show ip device tracking all</b>	Displays information about the entries in the IP device tracking table.

# ip device tracking

To enable IP device tracking, use the **ip device tracking** global configuration command. Use the **no** form of this command to disable this feature.

**ip device tracking**

**no ip device tracking**

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

**Command Default** IP device tracking is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
-----------------	---------	--------------

**Usage Guidelines** When IP device tracking is enabled, you can set the IP device tracking probe interval, count, and configure the ARP probe address with the **ip device tracking probe** command.

Use the **show ip device tracking all** command to display information about entries in the IP device tracking table. For more information about this command, see the Cisco IOS Security Command Reference, Release 12.4T.

**Examples** This example shows how to enable device tracking:

```
Switch(config)# ip device tracking
Switch(config)#

```

Related Commands	Command	Description
	<a href="#">ip device tracking probe</a>	Configures the IP device tracking table for ARP probes.
	<a href="#">show ip device tracking all</a>	Displays information about the entries in the IP device tracking table.

**ip dhcp snooping**

# ip dhcp snooping

Use the **ip dhcp snooping** global configuration command to globally enable DHCP snooping. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping**

**no ip dhcp snooping**

---

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

---

**Defaults** DHCP snooping is disabled.

---

**Command Modes** Global configuration

**Command History**

**Usage Guidelines** For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping.

DHCP snooping is not active until you enable snooping on a VLAN by using the **ip dhcp snooping vlan *vlan-id*** global configuration command.

---

**Examples** This example shows how to enable DHCP snooping:

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

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

**Related Commands**

Command	Description
<a href="#">ip dhcp snooping vlan</a>	Enables DHCP snooping on a VLAN.
<a href="#">show ip igmp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping binding

Use the **ip dhcp snooping binding** privileged EXEC command to configure the DHCP snooping binding database and to add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

**ip dhcp snooping binding** *mac-address vlan vlan-id ip-address interface interface-id expiry seconds*

**no ip dhcp snooping binding** *mac-address vlan vlan-id ip-address interface interface-id*

## Syntax Description

<i>mac-address</i>	Specify a MAC address.
<b>vlan</b> <i>vlan-id</i>	Specify a VLAN number. The range is 1 to 4094.
<i>ip-address</i>	Specify an IP address.
<b>interface</b> <i>interface-id</i>	Specify an interface on which to add or delete a binding entry.
<b>expiry</b> <i>seconds</i>	Specify the interval (in seconds) after which the binding entry is no longer valid. The range is 1 to 4294967295.

## Defaults

No default database is defined.

## Command Modes

Privileged EXEC

## Command History

### Usage Guidelines

Use this command when you are testing or debugging the switch.

In the DHCP snooping binding database, each database entry, also referred to as a binding, has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database can have up to 8192 bindings.

## Examples

This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface expiry 1000
```

## Related Commands

Command	Description
<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
<a href="#">show ip dhcp snooping binding</a>	Displays the dynamically configured bindings in the DHCP snooping binding database and the configuration information.
<a href="#">show ip source binding</a>	Displays the dynamically and statically configured bindings in the DHCP snooping binding database.

■ ip dhcp snooping binding

# ip dhcp snooping database

Use the **ip dhcp snooping database** global configuration command to configure the DHCP snooping binding database agent. Use the **no** form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.

```
ip dhcp snooping database { {flash:/filename | ftp://user:password@host/filename | http://[username:password]@[hostname | host-ip]/[directory]/image-name.tar | rcp://user@host/filename | tftp://host/filename} | timeout seconds | write-delay seconds}
no ip dhcp snooping database [timeout | write-delay]
```

Syntax Description	Note	Specify that the database agent or the binding file is in the flash memory.
<b>flash:/filename</b>		Specify that the database agent or the binding file is on an FTP server.
<b>http://[username:password]@[hostname   host-ip]/[directory]/image-name.tar</b>		Specify that the database agent or the binding file is on a TFTP server.
<b>rcp://user@host/filename</b>		Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.
<b>tftp://host/filename</b>		Specify that the database agent or the binding file is on a TFTP server.
<b>timeout seconds</b>		Specify (in seconds) how long to wait for the database transfer process to finish before stopping. The default is 300 seconds. The range is 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.
<b>write-delay seconds</b>		Specify (in seconds) the duration for which the transfer should be delayed after the binding database changes. The default is 300 seconds. The range is 15 to 86400.

## Defaults

The URL for the database agent or binding file is not defined.

The timeout value is 300 seconds (5 minutes).

The write-delay value is 300 seconds (5 minutes).

## Command Modes

Global configuration

## Command History

### Usage Guidelines

The DHCP snooping binding database can have up to 8192 bindings.

**ip dhcp snooping database**

To ensure that the lease time in the database is accurate, we recommend that Network Time Protocol (NTP) is enabled and configured for these features:

- NTP authentication
- NTP peer and server associations
- NTP broadcast service
- NTP access restrictions
- NTP packet source IP address

If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Because both NVRAM and the flash memory have limited storage capacities, we recommend that you store a binding file on a TFTP server. You must create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can first write bindings to the binding file at that URL.

Use the **ip dhcp snooping database flash:/filename** command to save the DHCP snooping binding database in the NVRAM.

If you set the **ip dhcp snooping database timeout** command to 0 seconds and the database is being written to a TFTP file, if the TFTP server goes down, the database agent continues to try the transfer indefinitely. No other transfer can be initiated while this one is in progress. This might be inconsequential because if the server is down, no file can be written to it.

Use the **no ip dhcp snooping database** command to disable the agent.

Use the **no ip dhcp snooping database timeout** command to reset the timeout value.

Use the **no ip dhcp snooping database write-delay** command to reset the write-delay value.

---

**Examples**

This example shows how to store a binding file at an IP address of 10.1.1.1 that is in a directory called *directory*. A file named *file* must be present on the TFTP server.

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

This example shows how to store a binding file called *file01.txt* in the NVRAM:

```
Switch(config)# ip dhcp snooping database flash:file01.txt
```

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

---

**Related Commands**

Command	Description
<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database.
<a href="#">show ip dhcp snooping database</a>	Displays the status of DHCP snooping database agent.

# ip dhcp snooping information option

Use the **ip dhcp snooping information option** global configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

**ip dhcp snooping information option**

**no ip dhcp snooping information option**

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

**Defaults** DHCP option-82 data is inserted.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, **vlan-mod-port**, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

### Examples

This example shows how to enable DHCP option-82 data insertion:

```
Switch(config)# ip dhcp snooping information option
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

### Related Commands

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

---

■ **ip dhcp snooping information option allow-untrusted**

# ip dhcp snooping information option allow-untrusted

Use the **ip dhcp snooping information option allow-untrusted** global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping information option allow-untrusted**

**no ip dhcp snooping information option allow-untrusted**

---

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

---

**Defaults** The switch drops DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch.

---

**Command Modes** Global configuration

---

**Command History**

**Usage Guidelines** You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the **ip dhcp snooping information option allow-untrusted** command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.




---

**Note** Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

---

**Examples**

This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

Related Commands	Command	Description
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

**ip dhcp snooping limit rate**

# ip dhcp snooping limit rate

Use the **ip dhcp snooping limit rate** interface configuration command to configure the number of DHCP messages an interface can receive per second. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping limit rate *rate***

**no ip dhcp snooping limit rate**

<b>Syntax Description</b>	<i>rate</i>	The number of DHCP messages an interface can receive per second. The range is 1 to 2048.
---------------------------	-------------	--

<b>Defaults</b>	DHCP snooping rate limiting is disabled.
-----------------	--

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

**Command History**

<b>Usage Guidelines</b>	Normally, the rate limit applies to untrusted interfaces. If you want to configure rate limiting for trusted interfaces, keep in mind that trusted interfaces might aggregate DHCP traffic on multiple VLANs (some of which might not be snooped) in the switch, and you will need to adjust the interface rate limits to a higher value.
-------------------------	---

If the rate limit is exceeded, the interface is error-disabled. If you enabled error recovery by entering the **errdisable recovery dhcp-rate-limit** global configuration command, the interface retries the operation again when all the causes have timed out. If the error-recovery mechanism is not enabled, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

<b>Examples</b>	This example shows how to set a message rate limit of 150 messages per second on an interface:
-----------------	--

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">errdisable recovery</a>	Configures the recover mechanism.
	<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
	<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

# ip dhcp snooping trust

Use the **ip dhcp snooping trust** interface configuration command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

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

**Defaults** DHCP snooping trust is disabled.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

Configure as trusted ports those that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

### Examples

This example shows how to enable DHCP snooping trust on a port:

```
Switch(config-if)# ip dhcp snooping trust
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

### Related Commands

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

---

■ **ip dhcp snooping verify**

# ip dhcp snooping verify

Use the **ip dhcp snooping verify** global configuration command to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to configure the switch to not verify the MAC addresses.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

---

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

---

**Defaults** The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

---

**Command Modes** Global configuration

---

**Command History**

**Usage Guidelines** In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

---

**Examples** This example shows how to disable the MAC address verification:

```
Switch(config)# no ip dhcp snooping verify mac-address
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

---

**Related Commands**

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

# ip dhcp snooping vlan

To enable DHCP snooping on a VLAN, use the **ip dhcp snooping vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**ip dhcp snooping vlan *vlan-range***

**no ip dhcp snooping vlan *vlan-range***

---

<b>Syntax Description</b>	<i>vlan-range</i>	Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping. The range is 1 to 4094.  You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
---------------------------	-------------------	---

---

**Defaults** DHCP snooping is disabled on all VLANs.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** You must first globally enable DHCP snooping by entering the **ip dhcp snooping** global configuration command before enabling DHCP snooping on a VLAN.

DHCP snooping intercepts and inspects DHCP packets entering untrusted ports and either forwards or drops the packets.

You can verify the configuration by entering the **show ip dhcp snooping** user EXEC command.

## Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch(config)# ip dhcp snooping vlan 10
```

## Related Commands

---

Command	Description
<b>ip dhcp snooping</b>	Globally enables DHCP snooping.
<b>show ip dhcp snooping</b>	Displays the DHCP snooping configuration.

---

---

■ **ip dhcp snooping vlan information option format-type circuit-id string**

# ip dhcp snooping vlan information option format-type circuit-id string

Use the **ip dhcp snooping vlan information option format-type circuit-id string** interface configuration command to configure the option-82 circuit-ID suboption. Use the **no** form of this command to configure the default circuit-ID suboption.

**ip dhcp snooping vlan *vlan-id* information option format-type circuit-id [override] string**  
*ASCII-string*

**no ip dhcp snooping vlan *vlan-id* information option format-type circuit-id [override] string**

<b>Syntax Description</b>	<table border="0"> <tr> <td><b>vlan <i>vlan-id</i></b></td><td>Specify the VLAN ID. The range is 1 to 4094.</td></tr> <tr> <td><b>override</b></td><td>(Optional) Specify an override string, using from 3 to 63 ASCII characters (no spaces).</td></tr> <tr> <td><b>string</b><i>ASCII-string</i></td><td>Specify a circuit ID, using from 3 to 63 ASCII characters (no spaces).</td></tr> </table>	<b>vlan <i>vlan-id</i></b>	Specify the VLAN ID. The range is 1 to 4094.	<b>override</b>	(Optional) Specify an override string, using from 3 to 63 ASCII characters (no spaces).	<b>string</b> <i>ASCII-string</i>	Specify a circuit ID, using from 3 to 63 ASCII characters (no spaces).
<b>vlan <i>vlan-id</i></b>	Specify the VLAN ID. The range is 1 to 4094.						
<b>override</b>	(Optional) Specify an override string, using from 3 to 63 ASCII characters (no spaces).						
<b>string</b> <i>ASCII-string</i>	Specify a circuit ID, using from 3 to 63 ASCII characters (no spaces).						

---

**Defaults** The switch VLAN and the port identifier, in the format **vlan-mod-port**, is the default circuit ID.

---

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(52)SE	The <b>override</b> keyword was added.

---

**Usage Guidelines** You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default circuit-ID suboption is the switch VLAN and the port identifier, in the format **vlan-mod-port**. This command allows you to configure a string of ASCII characters to be the circuit ID. When you want to override the **vlan-mod-port** format type and instead use the circuit-ID to define subscriber information, use the **override** keyword.




---

**Note** When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.

**Examples**

This example shows how to configure the option-82 circuit-ID suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

This example shows how to configure the option-82 circuit-ID override suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

**Note**

The **show ip dhcp snooping** user EXEC command only displays the global command output, including a remote-ID configuration. It does not display any per-interface, per-VLAN string that you have configured for the circuit ID.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

**ip igmp filter**

# ip igmp filter

Use the **ip igmp filter** interface configuration command to control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface. Use the **no** form of this command to remove the specified profile from the interface.

**ip igmp filter *profile number***

**no ip igmp filter**

---

<b>Syntax Description</b>	<i>profile number</i> The IGMP profile number to be applied. The range is 1 to 4294967295.
---------------------------	--

---

<b>Defaults</b>	No IGMP filters are applied.
-----------------	------------------------------

---

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

---

**Command History**

<b>Usage Guidelines</b>	You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to ports that belong to an EtherChannel group.  An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.
-------------------------	---

---

<b>Examples</b>	This example shows how to apply IGMP profile 22 to a port:
-----------------	--

```
Switch(config-if)# ip igmp filter 22
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp profile</a>	Configures the specified IGMP profile number.
	<a href="#">show ip dhcp snooping statistics</a>	Displays the characteristics of the specified IGMP profile.
	<a href="#">show running-config interface</a> <i>interface-id</i>	Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface.

---

# ip igmp max-groups

Use the **ip igmp max-groups** interface configuration command to set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table. Use the **no** form of this command to set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report.

**ip igmp max-groups {number | action {deny | replace}}**

**no ip igmp max-groups {number | action}**

## Syntax Description

<b>number</b>	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
<b>action deny</b>	When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action.
<b>action replace</b>	When the maximum number of entries is in the IGMP snooping forwarding table, replace the existing group with the new group for which the IGMP report was received.

## Defaults

The default maximum number of groups is no limit.

After the switch learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as **deny** and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.
- If you configure the throttling action as **replace** and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {deny | replace}** command has no effect.

**ip igmp max-groups****Examples**

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Switch(config-if)# ip igmp max-groups 25
```

This example shows how to configure the switch to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Switch(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config interface</b> <i>interface-id</i>	Displays the running configuration on the switch interface, including the maximum number of IGMP groups that an interface can join and the throttling action.

# ip igmp profile

Use the **ip igmp profile** global configuration command to create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switchport. Use the **no** form of this command to delete the IGMP profile.

**ip igmp profile *profile number***

**no ip igmp profile *profile number***

<b>Syntax Description</b>	<i>profile number</i> The IGMP profile number being configured. The range is 1 to 4294967295.
---------------------------	---

<b>Defaults</b>	No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.
-----------------	---

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

## Command History

<b>Usage Guidelines</b>	When you are in IGMP profile configuration mode, you can create the profile by using these commands:
	<ul style="list-style-type: none"> <li>• <b>deny</b>: specifies that matching addresses are denied; this is the default condition.</li> <li>• <b>exit</b>: exits from igmp-profile configuration mode.</li> <li>• <b>no</b>: negates a command or resets to its defaults.</li> <li>• <b>permit</b>: specifies that matching addresses are permitted.</li> <li>• <b>range</b>: specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.</li> </ul>

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

## Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

## Related Commands

**■ ip igmp profile**

Command	Description
<a href="#">ip igmp filter</a>	Applies the IGMP profile to the specified interface.
<a href="#">show ip dhcp snooping statistics</a>	Displays the characteristics of all IGMP profiles or the specified IGMP profile number.

# ip igmp snooping

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

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

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

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b>	(Optional) Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
---------------------------	----------------------------	---

**Defaults** IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

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

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

### Examples

This example shows how to globally enable IGMP snooping:

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

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

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

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

**ip igmp snooping**

Related Commands	Command	Description
	<a href="#"><b>ip igmp snooping report-suppression</b></a>	Enables IGMP report suppression.
	<a href="#"><b>show ip dhcp snooping statistics</b></a>	Displays the snooping configuration.
	<a href="#"><b>show ip igmp snooping groups</b></a>	Displays IGMP snooping multicast information.
	<a href="#"><b>show ip igmp snooping mrouter</b></a>	Displays the IGMP snooping router ports.
	<a href="#"><b>show ip igmp snooping querier</b></a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

# ip igmp snooping last-member-query-interval

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

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

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

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Enable IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094. <b><i>time</i></b> Interval time out in seconds. The range is 100 to 32768 milliseconds.
---------------------------	--

**Defaults**      The default timeout setting is 1000 milliseconds.

**Command Modes**      Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(46)SE	The range for <i>time</i> was modified to 100 to 32768 seconds.

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

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

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

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

The configuration is saved in NVRAM.

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

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

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

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

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

■ **ip igmp snooping last-member-query-interval**

Related Commands	Command	Description
	<a href="#"><b>ip igmp snooping</b></a>	Enables IGMP snooping on the switch or on a VLAN.
	<a href="#"><b>ip igmp snooping vlan immediate-leave</b></a>	Enables IGMP Immediate-Leave processing.
	<a href="#"><b>ip igmp snooping vlan mrouter</b></a>	Configures a Layer 2 port as a multicast router port.
	<a href="#"><b>ip igmp snooping vlan static</b></a>	Configures a Layer 2 port as a member of a group.
	<a href="#"><b>show ip igmp snooping</b></a>	Displays the IGMP snooping configuration.

# ip igmp snooping querier

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

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

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

Syntax Description	
<b>vlan <i>vlan-id</i></b>	(Optional) Enable IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
<b>address <i>ip-address</i></b>	(Optional) Specify a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
<b>max-response-time <i>response-time</i></b>	(Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
<b>query-interval <i>interval-count</i></b>	(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.
<b>tcn query[<b>count <i>count</i></b>   <b>interval <i>interval</i></b>]</b>	(Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings: <ul style="list-style-type: none"> <li><b>count <i>count</i></b>—Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.</li> <li><b>interval <i>interval</i></b>—Set the TCN query interval time. The range is 1 to 255.</li> </ul>
<b>timer expiry</b>	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
<b>version <i>version</i></b>	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.

## Defaults

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

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

## Command Modes

Global configuration

## Command History

## Usage Guidelines

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

**ip igmp snooping querier**

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

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

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

**Examples**

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

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

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

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

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

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

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

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

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

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

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

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

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

**Related Commands**

Command	Description
<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration.
<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.

# ip igmp snooping report-suppression

Use the **ip igmp snooping report-suppression** global configuration command to enable Internet Group Management Protocol (IGMP) report suppression. Use the **no** form of this command to disable IGMP report suppression and to forward all IGMP reports to multicast routers.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

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

**Defaults** IGMP report suppression is enabled.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

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

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

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

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

### Examples

This example shows how to disable report suppression:

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

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

### Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN.

**ip igmp snooping tcn**

# ip igmp snooping tcn

Use the **ip igmp snooping tcn** global configuration command to configure the Internet Group Management Protocol (IGMP) Topology Change Notification (TCN) behavior. Use the **no** form of this command to return to the default settings.

**ip igmp snooping tcn {flood query count *count* | query solicit}**

**no ip igmp snooping tcn {flood query count | query solicit}**

<b>Syntax Description</b>	<b>flood query count <i>count</i></b> Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10. <b>query solicit</b> Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event.
---------------------------	--

<b>Defaults</b>	The TCN flood query count is 2. The TCN query solicitation is disabled.
-----------------	--

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

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	Use <b>ip igmp snooping tcn flood query count</b> global configuration command to control the time that multicast traffic is flooded after a TCN event. If you set the TCN flood query count to 1 by using the <b>ip igmp snooping tcn flood query count</b> command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.
-------------------------	--

Use the **ip igmp snooping tcn query solicit** global configuration command to enable the switch to send the global leave message whether or not it is the spanning-tree root. This command also speeds the process of recovering from the flood mode caused during a TCN event.

<b>Examples</b>	This example shows how to specify 7 as the number of IGMP general queries for which the multicast traffic is flooded:
-----------------	---

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip igmp snooping</b>	Enables IGMP snooping on the switch or on a VLAN.
	<b>ip igmp snooping tcn flood</b>	Specifies flooding on an interface as the IGMP snooping spanning-tree TCN behavior.
	<b>show ip igmp snooping</b>	Displays the IGMP snooping configuration of the switch or the VLAN.



---

■ **ip igmp snooping tcn flood**

## ip igmp snooping tcn flood

Use the **ip igmp snooping tcn flood** interface configuration command to specify multicast flooding as the Internet Group Management Protocol (IGMP) snooping spanning-tree Topology Change Notification (TCN) behavior. Use the **no** form of this command to disable the multicast flooding.

**ip igmp snooping tcn flood**

**no ip igmp snooping tcn flood**

---

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

---

**Defaults** Multicast flooding is enabled on an interface during a spanning-tree TCN event.

---

**Command Modes** Interface configuration

---

**Command History**

**Usage Guidelines** When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, the flooding might exceed the capacity of the link and cause packet loss.

You can change the flooding query count by using the **ip igmp snooping tcn flood query count count** global configuration command.

---

**Examples** This example shows how to disable the multicast flooding on an interface:

Switch(config-if)# **no ip igmp snooping tcn flood**

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

---

Related Commands	Command	Description
	<b>ip igmp snooping</b>	Enables IGMP snooping on the switch or on a VLAN.
	<b>ip igmp snooping tcn</b>	Configures the IGMP TCN behavior on the switch.
	<b>show ip igmp snooping</b>	Displays the IGMP snooping configuration of the switch or the VLAN.

# ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping immediate-leave** global configuration command to enable Internet Group Management Protocol (IGMP) snooping immediate-leave processing on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

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

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

<b>Syntax Description</b>	<i>vlan-id</i>	Enable IGMP snooping and the Immediate-Leave feature on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
---------------------------	----------------	--

<b>Defaults</b>	IGMP immediate-leave processing is disabled.
-----------------	--

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

## Command History

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

You should configure the Immediate- Leave feature only when there is a maximum of one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The Immediate-Leave feature is supported only with IGMP Version 2 hosts.

## Examples

This example shows how to enable IGMP immediate-leave processing on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

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

## Related Commands

Command	Description
<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
<a href="#">show ip igmp snooping</a>	Displays the snooping configuration.
<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.
<a href="#">show ip igmp snooping querier</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

---

 ■ ip igmp snooping vlan mrouter

# ip igmp snooping vlan mrouter

Use the **ip igmp snooping mrouter** global configuration command to add a multicast router port or to configure the multicast learning method. Use the **no** form of this command to return to the default settings.

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

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

Syntax Description	<p><b>vlan-id</b></p> <p>Enable IGMP snooping, and add the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094.</p>
<b>interface <i>interface-id</i></b>	Specify the next-hop interface to the multicast router. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>fastethernet <i>interface number</i></b>—a Fast Ethernet IEEE 802.3 interface.</li> <li>• <b>gigabitethernet <i>interface number</i></b>—a Gigabit Ethernet IEEE 802.3z interface.</li> <li>• <b>port-channel <i>interface number</i></b>—a channel interface. The range is 0 to .</li> </ul>
<b>learn {cgmp   pim-dvmrp}</b>	Specify the multicast router learning method. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>cgmp</b>—Set the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets.</li> <li>• <b>pim-dvmrp</b>—Set the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets.</li> </ul>

---

## Defaults

By default, there are no multicast router ports.

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

---

## Command Modes

Global configuration

---

## Command History

### Usage Guidelines

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

The CGMP learn method is useful for reducing control traffic.

The configuration is saved in NVRAM.

---

## Examples

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

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

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

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

Related Commands	Command	Description
	<a href="#">ip igmp snooping report-suppression</a>	Enables IGMP report suppression.
	<a href="#">show ip igmp snooping</a>	Displays the snooping configuration.
	<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information.
	<a href="#">show ip igmp snooping mrouter</a>	Displays the IGMP snooping router ports.
	<a href="#">show ip igmp snooping querier</a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

---

■ **ip igmp snooping vlan static**

# ip igmp snooping vlan static

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

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

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

Syntax Description	<p><b>vlan-id</b> Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.</p> <p><b>ip-address</b> Add a Layer 2 port as a member of a multicast group with the specified group IP address.</p> <p><b>interface <i>interface-id</i></b> Specify the interface of the member port. The keywords have these meanings:</p> <ul style="list-style-type: none"> <li>• <b>fastethernet <i>interface number</i></b>—a Fast Ethernet IEEE 802.3 interface.</li> <li>• <b>gigabitethernet <i>interface number</i></b>—a Gigabit Ethernet IEEE 802.3z interface.</li> <li>• <b>port-channel <i>interface number</i></b>—a channel interface. The range is 0 to .</li> </ul>
--------------------	--

<b>Defaults</b>	By default, there are no ports statically configured as members of a multicast group.
-----------------	---

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

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.
-------------------------	---

The configuration is saved in NVRAM.

<b>Examples</b>	This example shows how to statically configure a host on an interface:
-----------------	--

```
Switch(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet0/1
Configuring port gigabitethernet0/1 on group 0100.5e02.0203
```

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

Related Commands	Command	Description
	<b>ip igmp snooping report-suppression</b>	Enables IGMP report suppression.
	<b>show ip igmp snooping</b>	Displays the snooping configuration.
	<b>show ip igmp snooping groups</b>	Displays IGMP snooping multicast information.

Command	Description
<b>show ip igmp snooping mrouter</b>	Displays the IGMP snooping router ports.
<b>show ip igmp snooping querier</b>	Displays the configuration and operation information for the IGMP querier configured on a switch.

**ip source binding**

# ip source binding

Use the **ip source binding** global configuration command to configure static IP source bindings on the switch. Use the **no** form of this command to delete static bindings.

**ip source binding mac-address vlan vlan-id ip-address interface interface-id**

**no source binding mac-address vlan vlan-id ip-address interface interface-id**

**Syntax Description**

<b>mac-address</b>	Specify a MAC address.
<b>vlan vlan-id</b>	Specify a VLAN number. The range is from 1 to 4094.
<b>ip-address</b>	Specify an IP address.
<b>interface interface-id</b>	Specify an interface on which to add or delete an IP source binding.

**Defaults**

No IP source bindings are configured.

**Command Modes**

Global configuration

**Command History****Usage Guidelines**

A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number. The entry is based on the MAC address and the VLAN number. If you modify an entry by changing only the IP address, the switch updates the entry instead creating a new one.

**Examples**

This example shows how to add a static IP source binding:

```
Switch(config)# ip source binding 0001.1234.1234 vlan 1 172.20.50.5 interface
```

This example shows how to add a static binding and then modify the IP address for it:

```
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.25 interface
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">ip verify source</a>	Enables IP source guard on an interface.
<a href="#">show ip source binding</a>	Displays the IP source bindings on the switch.
<a href="#">show ip verify source</a>	Displays the IP source guard configuration on the switch or on a specific interface.

# ip ssh

Use the **ip ssh** global configuration command to configure the switch to run Secure Shell (SSH) Version 1 or SSH Version 2. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting.

**ip ssh version [1 | 2]**

**no ip ssh version [1 | 2]**

---

## Syntax Description

- |          |   |
|----------|---|
| <b>1</b> | (Optional) Configure the switch to run SSH Version 1 (SSHv1). |
| <b>2</b> | (Optional) Configure the switch to run SSH Version 2 (SSHv2). |
- 

---

## Defaults

The default version is the latest SSH version supported by the SSH client.

---

## Command Modes

Global configuration

---

## Command History

### Usage Guidelines

If you do not enter this command or if you do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

The switch supports an SSHv1 or an SSHv2 server. It also supports an SSHv1 client. For more information about the SSH server and the SSH client, see the software configuration guide for this release.

A Rivest, Shamir, and Adelman (RSA) key pair generated by an SSHv1 server can be used by an SSHv2 server and the reverse.

---

## Examples

This example shows how to configure the switch to run SSH Version 2:

```
Switch(config)# ip ssh version 2
```

You can verify your settings by entering the **show ip ssh** or **show ssh** privileged EXEC command.

---

## Related Commands

Command	Description
<b>show ip ssh</b>	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server.
<b>show ssh</b>	Displays the status of the SSH server.

---

# ip verify source

Use the **ip verify source** interface configuration command to enable IP source guard on an interface. Use the **no** form of this command to disable IP source guard.

**ip verify source [port-security]**

**no ip verify source**

---

<b>Syntax Description</b>	<b>port-security</b>	(Optional) Enable IP source guard with IP and MAC address filtering. If you do not enter the <b>port-security</b> keyword, IP source guard with IP address filtering is enabled.
---------------------------	----------------------	---

---

<b>Defaults</b>	IP source guard is disabled.
-----------------	------------------------------

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

## Command History

<b>Usage Guidelines</b>	To enable IP source guard with source IP address filtering, use the <b>ip verify source</b> interface configuration command.  To enable IP source guard with source IP and MAC address filtering, use the <b>ip verify source port-security</b> interface configuration command.  To enable IP source guard with source IP and MAC address filtering, you must enable port security on the interface.
-------------------------	---

<b>Examples</b>	This example shows how to enable IP source guard with source IP address filtering:  Switch(config-if)# <b>ip verify source</b>  This example shows how to enable IP source guard with source IP and MAC address filtering: Switch(config-if)# <b>ip verify source port-security</b>  You can verify your settings by entering the <b>show ip source binding</b> privileged EXEC command.
-----------------	---

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>ip source binding</b></a>	Configures static bindings on the switch.
	<a href="#"><b>show ip verify source</b></a>	Displays the IP source guard configuration on the switch or on a specific interface.

---

**■ ipv6 mld snooping**

# ipv6 mld snooping

Use the **ipv6 mld snooping** global configuration command without keywords to enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping globally or on the specified VLAN. Use the **no** form of this command to disable MLD snooping on the switch or switch stack or the VLAN.

**ipv6 mld snooping [vlan *vlan-id*]**

**no ipv6 mld snooping [vlan *vlan-id*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b>	(Optional) Enable or disable IPv6 MLD snooping on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.
---------------------------	----------------------------	--

<b>Defaults</b>	MLD snooping is globally disabled on the switch. MLD snooping is enabled on all VLANs. However, MLD snooping must be globally enabled before VLAN snooping will take place.
-----------------	--

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

<b>Command History</b>	
<b>Usage Guidelines</b>	To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6</b> global configuration command and reload the switch.

When MLD snooping is globally disabled, it is disabled on all the existing VLAN interfaces. When you globally enable MLD snooping, it is enabled on all VLAN interfaces that are in the default state (enabled). VLAN configuration will override global configuration on interfaces on which MLD snooping has been disabled.

If MLD snooping is globally disabled, you cannot enable it on a VLAN. If MLD snooping is globally enabled, you can disable it on individual VLANs.

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

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

<b>Examples</b>	This example shows how to globally enable MLD snooping:
-----------------	---

```
Switch(config)# ipv6 mld snooping
```

This example shows how to disable MLD snooping on a VLAN:

```
Switch(config)# no ipv6 mld snooping vlan 11
```

You can verify your settings by entering the **show ipv6 mld snooping** user EXEC command.

Related Commands	Command	Description
	<b>sdm prefer</b>	Configures an SDM template to optimize system resources based on how the switch is being used.
	<b>show ipv6 mld snooping</b>	Displays MLD snooping configuration.

**■ ipv6 mld snooping last-listener-query-count**

# ipv6 mld snooping last-listener-query-count

Use the **ipv6 mld snooping last-listener-query-count** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery Multicast Address Specific Queries (MASQs) or that will be sent before aging out a client. Use the **no** form of this command to reset the query count to the default settings.

```
ipv6 mld snooping [vlan vlan-id] last-listener-query-count integer_value
no ipv6 mld snooping [vlan vlan-id] last-listener-query-count
```

<b>Syntax Description</b>	<b>vlan vlan-id</b> (Optional) Configure last-listener query count on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. <b>integer_value</b> The range is 1 to 7.
---------------------------	---

<b>Command Default</b>	The default global count is 2. The default VLAN count is 0 (the global count is used).
------------------------	---

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

**Command History**

**Usage Guidelines** To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

In MLD snooping, the IPv6 multicast router periodically sends out queries to hosts belonging to the multicast group. If a host wants to leave a multicast group, it can silently leave or it can respond to the query with a Multicast Listener Done message (equivalent to an IGMP Leave message). When Immediate Leave is not configured (which it should not be if multiple clients for a group exist on the same port), the configured last-listener query count determines the number of MASQs that are sent before an MLD client is aged out.

When the last-listener query count is set for a VLAN, this count overrides the value configured globally. When the VLAN count is not configured (set to the default of 0), the global count is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

**Examples**

This example shows how to globally set the last-listener query count:

```
Switch(config)# ipv6 mld snooping last-listener-query-count 1
```

This example shows how to set the last-listener query count for VLAN 10:

```
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
```

You can verify your settings by entering the **show ipv6 mld snooping [vlan vlan-id]** user EXEC command.

Related Commands	Command	Description
	<a href="#">ipv6 mld snooping last-listener-query-interval</a>	Sets IPv6 MLD snooping last-listener query interval.
	<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
	<a href="#">show ipv6 mld snooping querier</a>	Displays MLD snooping configuration.

---

 ■ **ipv6 mld snooping last-listener-query-interval**

# ipv6 mld snooping last-listener-query-interval

Use the **ipv6 mld snooping last-listener-query-interval** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping last-listener query interval on the switch or on a VLAN. This time interval is the maximum time that a multicast router waits after issuing a Multicast Address Specific Query (MASQ) before deleting a port from the multicast group. Use the **no** form of this command to reset the query time to the default settings.

**ipv6 mld snooping [vlan *vlan-id*] last-listener-query-interval *integer\_value***

**no ipv6 mld snooping [vlan *vlan-id*] last-listener-query-interval**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Configure last-listener query interval on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. <b>integer_value</b> Set the time period (in thousands of a second) that a multicast router to wait after issuing a MASQ before deleting a port from the multicast group. The range is 100 to 32,768. The default is 1000 (1 second),
---------------------------	---

**Command Default** The default global query interval (maximum response time) is 1000 (1 second).

The default VLAN query interval (maximum response time) is 0 (the global count is used).

**Command Modes** Global configuration

## Command History

### Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

In MLD snooping, when the IPv6 multicast router receives an MLD leave message, it sends out queries to hosts belonging to the multicast group. If there are no responses from a port to a MASQ for a length of time, the router deletes the port from the membership database of the multicast address. The last listener query interval is the maximum time that the router waits before deleting a nonresponsive port from the multicast group.

When a VLAN query interval is set, this overrides the global query interval. When the VLAN interval is set at 0, the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

---

### Examples

This example shows how to globally set the last-listener query interval to 2 seconds:

```
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
```

This example shows how to set the last-listener query interval for VLAN 1 to 5.5 seconds:

```
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
```

You can verify your settings by entering the **show ipv6 MLD snooping [vlan *vlan-id*]** user EXEC command.

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping last-listener-query-count</a>	Sets IPv6 MLD snooping last-listener query count.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#">show ipv6 mld snooping querier</a>	Sets IPv6 MLD snooping last-listener query interval.

**■ ipv6 mld snooping listener-message-suppression**

# ipv6 mld snooping listener-message-suppression

Use the **ipv6 mld snooping listener-message-suppression** global configuration command to enable IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping listener message suppression. Use the **no** form of this command to disable MLD snooping listener message suppression.

**ipv6 mld snooping listener-message-suppression**

**no ipv6 mld snooping listener-message-suppression**

**Command Default** The default is for MLD snooping listener message suppression to be disabled.

**Command Modes** Global configuration

**Command History**

**Usage Guidelines** To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

MLD snooping listener message suppression is equivalent to IGMP snooping report suppression. When enabled, received MLDv1 reports to a group are forwarded to IPv6 multicast routers only once in every report-forward time. This prevents the forwarding of duplicate reports.

**Examples** This example shows how to enable MLD snooping listener-message-suppression:

```
Switch(config)# ipv6 mld snooping listener-message-suppression
```

This example shows how to disable MLD snooping listener-message-suppression:

```
Switch(config)# no ipv6 mld snooping listener-message-suppression
```

You can verify your settings by entering the **show ipv6 mld snooping [vlan vlan-id]** user EXEC command.

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables IPv6 MLD snooping.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#">show ipv6 mld snooping</a>	Displays MLD snooping configuration.

# ipv6 mld snooping robustness-variable

Use the **ipv6 mld snooping robustness-variable** global configuration command to configure the number of IP version 6 (IPv6) Multicast Listener Discovery (MLD) queries that the switch sends before deleting a listener that does not respond, or enter a VLAN ID to configure on a per-VLAN basis. Use the **no** form of this command to reset the variable to the default settings.

```
ipv6 mld snooping [vlan vlan-id] robustness-variable integer_value
no ipv6 mld snooping [vlan vlan-id] robustness-variable
```

<b>Syntax Description</b>	<b>vlan vlan-id</b> (Optional) Configure the robustness variable on the specified VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. <b>integer_value</b> The range is 1 to 3.
---------------------------	---

**Command Default** The default global robustness variable (number of queries before deleting a listener) is 2.

The default VLAN robustness variable (number of queries before aging out a multicast address) is 0, which means that the system uses the global robustness variable for aging out the listener.

**Command Modes** Global configuration

## Command History

## Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

Robustness is measured in terms of the number of MLDv1 queries sent with no response before a port is removed from a multicast group. A port is deleted when there are no MLDv1 reports received for the configured number of MLDv1 queries. The global value determines the number of queries that the switch waits before deleting a listener that does not respond and applies to all VLANs that do not have a VLAN value set.

The robustness value configured for a VLAN overrides the global value. If the VLAN robustness value is 0 (the default), the global value is used.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

## Examples

This example shows how to configure the global robustness variable so that the switch sends out three queries before it deletes a listener port that does not respond:

```
Switch(config)# ipv6 mld snooping robustness-variable 3
```

This example shows how to configure the robustness variable for VLAN 1. This value overrides the global configuration for the VLAN:

```
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
```

**■ ipv6 mld snooping robustness-variable**

You can verify your settings by entering the **show ipv6 MLD snooping [vlan *vlan-id*]** user EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>ipv6 mld snooping last-listener-query-count</b></a>	Sets IPv6 MLD snooping last-listener query count.
<a href="#"><b>sdm prefer</b></a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#"><b>show ipv6 mld snooping</b></a>	Displays MLD snooping configuration.

# ipv6 mld snooping tcn

Use the **ipv6 mld snooping tcn** global configuration commands to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) Topology Change Notifications (TCNs). Use the **no** form of the commands to reset the default settings.

**ipv6 mld snooping tcn {flood query count *integer\_value* | query solicit}**

**no ipv6 mld snooping tcn {flood query count *integer\_value* | query solicit}**

<b>Syntax Description</b>	<b>flood query count <i>integer_value</i></b> Set the flood query count, which is the number of queries that are sent before forwarding multicast data to only those ports requesting to receive it. The range is 1 to 10. <b>query solicit</b> Enable soliciting of TCN queries.
---------------------------	--

<b>Command Default</b>	TCN query soliciting is disabled. When enabled, the default flood query count is 2.
------------------------	--

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

## Command History

<b>Usage Guidelines</b>	To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6</b> global configuration command and reload the switch.
-------------------------	--

<b>Examples</b>	This example shows how to enable TCN query soliciting:
-----------------	--

```
Switch(config)# ipv6 mld snooping tcn query solicit.
```

This example shows how to set the flood query count to 5:

```
Switch(config)# ipv6 mld snooping tcn flood query count 5.
```

You can verify your settings by entering the **show ipv6 MLD snooping [vlan *vlan-id*]** user EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sdm prefer</b>	Configures an SDM template to optimize system resources based on how the switch is being used.
	<b>show ipv6 mld snooping</b>	Displays MLD snooping configuration.

**■ ipv6 mld snooping vlan**

# ipv6 mld snooping vlan

Use the **ipv6 mld snooping vlan** global configuration command to configure IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping parameters on the VLAN interface. Use the **no** form of this command to reset the parameters to the default settings.

**ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-multicast-address* **interface** *interface-id*]**

**no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]**

<b>Syntax Description</b>	
<b>vlan <i>vlan-id</i></b>	Specify a VLAN number. The range is 1 to 1001 and 1006 to 4094.
<b>immediate-leave</b>	(Optional) Enable MLD Immediate-Leave processing on a VLAN interface. Use the <b>no</b> form of the command to disable the Immediate Leave feature on the interface.
<b>mrouter interface</b>	(Optional) Configure a multicast router port. The <b>no</b> form of the command removes the configuration.
<b>static <i>ip6-multicast-address</i></b>	(Optional) Configure a multicast group with the specified IPv6 multicast address.
<b>interface <i>interface-id</i></b>	Add a Layer 2 port to the group. The mrouter or static interface can be a physical port or a <b>port-channel</b> interface in the range of 1 to 48.

**Command Default** MLD snooping Immediate-Leave processing is disabled.

By default, there are no static IPv6 multicast groups.

By default, there are no multicast router ports.

**Command Modes** Global configuration

**Command History**

**Usage Guidelines**

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

You should only configure the Immediate-Leave feature when there is only one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The **static** keyword is used for configuring the MLD member ports statically.

The configuration and the static ports and groups are saved in NVRAM.

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

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

**Examples**

This example shows how to enable MLD Immediate-Leave processing on VLAN 1:

```
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
```

This example shows how to disable MLD Immediate-Leave processing on VLAN 1:

```
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
```

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

```
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/01/2
```

This example shows how to configure a static multicast group:

```
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/01/2
```

You can verify your settings by entering the **show ipv6 mld snooping vlan *vlan-id*** user EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>ipv6 mld snooping</b></a>	Enables IPv6 MLD snooping.
<a href="#"><b>ipv6 mld snooping vlan</b></a>	Configures IPv6 MLD snooping on the VLAN.
<a href="#"><b>sdm prefer</b></a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#"><b>show ipv6 mld snooping</b></a>	Displays IPv6 MLD snooping configuration.

**lacp port-priority**

# lacp port-priority

Use the **lacp port-priority** interface configuration command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

**lacp port-priority** *priority*

**no lacp port-priority**

<b>Syntax Description</b>	<i>priority</i>	Port priority for LACP. The range is 1 to 65535.
---------------------------	-----------------	--

<b>Defaults</b>	The default is 32768.
-----------------	-----------------------

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

<b>Command History</b>	
------------------------	--

**Usage Guidelines** The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically *lower* value has a *higher* priority: When there are more than eight ports in an LACP channel-group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535) an internal value for the port number determines the priority.



**Note** The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lacp system-priority** global configuration command for determining which switch controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

---

**Examples**

This example shows how to configure the LACP port priority on a port:

```
Switch(config-if)# lacp port-priority 1000
```

You can verify your settings by entering the **show lacp [channel-group-number] internal** privileged EXEC command.

---

**Related Commands**

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#">lacp system-priority</a>	Configures the LACP system priority.
<a href="#">show lacp [channel-group-number]</a> <b>internal</b>	Displays internal information for all channel groups or for the specified channel group.

---

**lacp system-priority**

# lacp system-priority

Use the **lacp system-priority** global configuration command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

**lacp system-priority** *priority*

**no lacp system-priority**

<b>Syntax Description</b>	<i>priority</i>	System priority for LACP. The range is 1 to 65535.
---------------------------	-----------------	--

<b>Defaults</b>	The default is 32768.
-----------------	-----------------------

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

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	The <b>lacp system-priority</b> command determines which switch in an LACP link controls port priorities. An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel-group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.
-------------------------	--

In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

For more information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

<b>Examples</b>	This example shows how to set the LACP system priority:
-----------------	---

```
Switch(config)# lacp system-priority 20000
```

You can verify your settings by entering the **show lacp sys-id** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">channel-group</a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#">lacp port-priority</a>	Configures the LACP port priority.
<a href="#">show lacp sys-id</a>	Displays the system identifier that is being used by LACP.

**link state group**

# link state group

Use the **link state group** interface configuration command to configure a port as a member of a link-state group. Use the **no** form of this command to remove the port from the link-state group.

**link state group [number] {upstream | downstream}**

**no link state group [number] {upstream | downstream}**

<b>Syntax Description</b>	<b>number</b>	(Optional) Specify the link-state group number. The group number can be 1 to .The default is 1.
	<b>upstream</b>	Configure a port as an upstream port for a specific link-state group.
	<b>downstream</b>	Configure a port as a downstream port for a specific link-state group.

**Defaults** The default group is group 1.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

**Usage Guidelines** Use the **link state group** interface configuration command to configure a port as an upstream or downstream interface for the specified link-state group. If the group number is omitted, the default group number is 1.

To enable link-state tracking, create a *link-state group*, and specify the interfaces that are assigned to the link-state group. An interface can be an aggregation of ports (an EtherChannel), a single physical port in access or trunk mode, or a routed port. In a link-state group, these interfaces are bundled together. The *downstream interfaces* are bound to the *upstream interfaces*. Interfaces connected to servers are referred to as downstream interfaces, and interfaces connected to distribution switches and network devices are referred to as upstream interfaces.

For more information about the interactions between the downstream and upstream interfaces, see the “Configuring EtherChannels and Link-State Tracking” chapter of the software configuration guide for this release.

Follow these guidelines to avoid configuration problems:

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- An interface cannot be a member of more than one link-state group.

---

**Examples**

This example shows how to configure the interfaces as **upstream** in group 2:

```
Switch# configure terminal
Switch(config-if-range)# link state group 2 downstream
Switch(config-if-range)# end
Switch(config-if)# end
```

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

---

**Related Commands**

Command	Description
<a href="#">link state track</a>	Enables a link-state group.
<a href="#">show link state group</a>	Displays the link-state group information.
<a href="#">show running-config</a>	Displays the current operating configuration.

---

**link state track**

# link state track

Use the **link state track** user EXEC command to enable a link-state group. Use the **no** form of this command to disable a link-state group.

**link state track [number]**

**no link state track [number]**

<b>Syntax Description</b>	<i>number</i>	(Optional) Specify the link-state group number. The group number can be 1 to . The default is 1.
---------------------------	---------------	--

<b>Defaults</b>	Link-state tracking is disabled for all groups.
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>link state track</b> global configuration command to enable a link-state group.
-------------------------	--

<b>Examples</b>	This example shows how enable link-state group 2:
-----------------	---

```
Switch(config)# link state track 2
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>link state track</b>	Configures an interface as a member of a link-state group.
	<b>show link state group</b>	Displays the link-state group information.
	<b>show running-config</b>	Displays the current operating configuration.

# location (global configuration)

Use the **location** global configuration command to configure location information for an endpoint. Use the **no** form of this command to remove the location information.

```
location {admin-tag string | civic-location identifier id | elin-location string identifier id}
no location {admin-tag string | civic-location identifier id | elin-location string identifier id}
```

Syntax Description	<b>admin-tag</b> Configure administrative tag or site information. <b>civic-location</b> Configure civic location information. <b>elin-location</b> Configure emergency location information (ELIN). <b>identifier id</b> Specify the ID for the civic location or the elin location. The ID range is 1 to 4095. <b>Note</b> The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes. <b>string</b> Specify the site or location information in alphanumeric format.
--------------------	---

**Defaults** This command has no default setting.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(40)SE	This command was introduced.

**Usage Guidelines** After entering the **location civic-location identifier id** global configuration command, you enter civic location configuration mode. In this mode, you can enter the civic location and the postal location information.

The civic-location identifier must not exceed 250 bytes.

Use the **no lldp med-tlv-select location** information interface configuration command to disable the location TLV. The location TLV is enabled by default. For more information, see the “Configuring LLDP and LLDP-MED” chapter of the software configuration guide for this release.

**location (global configuration)****Examples**

This example shows how to configure civic location information on the switch:

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command. This example shows how to configure the emergency location information on the switch:

```
Switch (config)# location elin-location 14085553881 identifier 1
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">location (interface configuration)</a>	Configures the location information for an interface.
<a href="#">show location</a>	Displays the location information for an endpoint.

# location (interface configuration)

Use the **location** interface command to enter location information for an interface. Use the **no** form of this command to remove the interface location information.

**location { additional-location-information word | civic-location-id id | elin-location-id id }**

**no location { additional-location-information word | civic-location-id id | elin-location-id id }**

Syntax Description	<b>additional-location-information</b>	Configure additional information for a location or place.
<i>word</i>		Specify a word or phrase that provides additional location information.
<b>civic-location-id</b>		Configure global civic location information for an interface.
<b>elin-location-id</b>		Configure emergency location information for an interface.
<i>id</i>		Specify the ID for the civic location or the elin location. The ID range is 1 to 4095.
	<b>Note</b>	The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location ID does not exceed 250 bytes.

**Defaults** This command has no default setting.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(40)SE	This command was introduced.

**Usage Guidelines** After entering the **location civic-location-id id** interface configuration command, you enter civic location configuration mode. In this mode, you can enter the additional location information. The civic-location identifier must not exceed 250 bytes. You can verify your settings by entering the **show location civic interface** privileged EXEC command.

**Examples** These examples show how to enter civic location information for an interface:

```
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

This example shows how to enter emergency location information for an interface:

```
Switch(config-if)# location elin-location-id 1
```

**■ location (interface configuration)**

```
Switch(config-if)# end
```

Related Commands	Command	Description
	<a href="#">location (global configuration)</a>	Configures the location information for an endpoint.
	<a href="#">show location</a>	Displays the location information for an endpoint.

# logging event

Use the **logging event** interface configuration command to enable notification of interface link status changes. Use the **no** form of this command to disable notification.

```
logging event {bundle-status | link-status | spanning-tree | status | trunk status}
```

```
no logging event {bundle-status | link-status | spanning-tree | status | trunk status}
```

<b>Syntax Description</b>	<b>bundle-status</b> Enable notification of BUNDLE and UNBUNDLE messages. <b>link-status</b> Enable notification of interface data link status changes. <b>spanning-tree</b> Enable notification of spanning-tree events. <b>status</b> Enable notification of spanning-tree state change messages. <b>trunk-status</b> Enable notification of trunk-status messages.
---------------------------	---

**Defaults** Event logging is disabled.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
------------------------	----------------	---------------------

**Examples** This example shows how to enable spanning-tree logging:

```
Switch(config-if)# logging event spanning-tree
```

---

 logging event power-inline-status

# logging event power-inline-status

Use the **logging event power-inline-status** interface configuration command to enable the logging of Power over Ethernet (PoE) events. Use the **no** form of this command to disable the logging of PoE status events; however, the **no** form of this command does not disable PoE error events.

**logging event power-inline-status**

**no logging event power-inline-status**

---

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

---

**Defaults** Logging of PoE events is enabled.

---

**Command Modes** Interface configuration

---

**Command History**

**Usage Guidelines** The **logging event power-inline-status** command is available only on PoE interfaces.

---

**Examples** This example shows how to enable logging of PoE events on a port:

```
Switch(config-if)# interface
Switch(config-if)# logging event power-inline-status
Switch(config-if)#

```

---

**Related Commands**

Command	Description
<a href="#">power inline</a>	Configures the power management mode for the specified PoE port or for all PoE ports.
<a href="#">show controllers</a> <a href="#">power inline</a>	Displays the values in the registers of the specified PoE controller.

# logging file

Use the **logging file** global configuration command to set logging file parameters. Use the **no** form of this command to return to the default setting.

**logging file** *filesystem:filename* [*max-file-size* | **nomax** [*min-file-size*]] [*severity-level-number* | *type*]

**no logging file** *filesystem:filename* [*severity-level-number* | *type*]

Syntax Description	<i>filesystem:filename</i>	Alias for a flash file system. Contains the path and name of the file that contains the log messages.
		<b>Note</b> The syntax for the local flash file system: <b>flash:</b>
	<i>max-file-size</i>	(Optional) Specify the maximum logging file size. The range is 4096 to 2147483647.
	<b>nomax</b>	(Optional) Specify the maximum file size of 2147483647.
	<i>min-file-size</i>	(Optional) Specify the minimum logging file size. The range is 1024 to 2147483647.
	<i>severity-level-number</i>	(Optional) Specify the logging severity level. The range is 0 to 7. See the <i>type</i> option for the meaning of each level.
	<i>type</i>	(Optional) Specify the logging type. These keywords are valid: <ul style="list-style-type: none"> <li>• <b>emergencies</b>—System is unusable (severity 0).</li> <li>• <b>alerts</b>—Immediate action needed (severity 1).</li> <li>• <b>critical</b>—Critical conditions (severity 2).</li> <li>• <b>errors</b>—Error conditions (severity 3).</li> <li>• <b>warnings</b>—Warning conditions (severity 4).</li> <li>• <b>notifications</b>—Normal but significant messages (severity 5).</li> <li>• <b>informational</b>—Information messages (severity 6).</li> <li>• <b>debugging</b>—Debugging messages (severity 7).</li> </ul>

## Defaults

The minimum file size is 2048 bytes; the maximum file size is 4096 bytes.

The default severity level is 7 (**debugging** messages and numerically lower levels).

## Command Modes

Global configuration

## Command History

### Usage Guidelines

After saving the log to flash memory by using the **logging file flash:filename** global configuration command, you can use the **more flash:filename** privileged EXEC command to display its contents.

**logging file**

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

**Examples**

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the running configuration on the switch.

# mab request format attribute 1

To configure a MAB username, use the **mab request format attribute 1** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
mab request format attribute 1 groupsize {1 | 2 | 4 | 12} separator{- | : | .} {lowercase | uppercase}
```

Syntax Description	<b>groupsize</b>	Specifies the number of hex nibbles to concatenate before insertion of a separator.
	<b>{1   2   4   12}</b>	A group size must be either 1, 2, 4, or 12.
	<b>separator</b>	Specifies the character that separates the hex nibbles according to groupsize.
	<b>-   :   .</b>	A separator must be either a hyphen, colon, or period.
	<b>lowercase   uppercase</b>	Specifies whether non-numeric hex nibbles should be in lowercase or uppercase.

## Defaults

groupsize: 12  
case: lowercase  
separator: None

## Command Modes

Global configuration (config)

## Command History

Release	Modification
15.0(2) SE	This command was introduced.

## Usage Guidelines

The **mab request format attribute 1** command controls the format of the MAC address as presented in the User-Name field of the MAB access request packet. The specified format applies to every future authentication on every interface, but does not affect existing authenticated sessions.

## Examples

The following table shows resulting User-Name customization examples based on various combinations of the **groupsize** and **separator** values.

groupsize	separator	Resulting Format of User-Name Attribute
1	:	0:8:0:0:2:b:8:6:1:9:d:e
2	-	08-00-2b-86-19-de
4	.	0800.2b86.19de
12	None	08002b8619de

**mab request format attribute 1**

Related Commands	Command	Description
	<b>mab</b>	Enables MAC authentication bypass on a port.
	<b>mab eap</b>	Configures a port to use Extensible Authentication Protocol (EAP).
	<b>mab request format attribute 2</b>	Specifies a custom password value for the User-Password attribute in MAB-generated Access-Request packets.
	<b>mab request format attribute 32</b>	Enables VLAN ID-based MAC authentication on a switch.

# mab request format attribute 2

To configure a MAB password, use the **mab request format attribute 2** command in global configuration mode. Use the **no** form of this command to return to the default setting.

**mab request format attribute 2 {0 | 7} <LINE>**

<b>Syntax Description</b>	<b>0</b> Specifies a cleartext password. <b>7</b> Specifies an encrypted password. <b>LINE</b> Specifies the password to be used in the User-Password attribute.
---------------------------	--

<b>Defaults</b>	<i>LINE</i> : username
-----------------	------------------------

<b>Command Modes</b>	Global configuration (config)
----------------------	-------------------------------

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

<b>Usage Guidelines</b>	The <b>mab request format attribute 2</b> command specifies a custom password value for the User-Password attribute in MAB-generated Access-Request packets. The password scope is global; that is, it applies to every authentication on every interface. If you do not specify a password, the password is the same as the username including any applied formatting.
-------------------------	---

<b>Examples</b>	The following table shows password examples based on username format:
-----------------	---

<b>MAC</b>	<b>Username Format</b>	<b>Supplied Password</b>	<b>Resulting Password</b>
08002b8619de	(2, -)	None	08-00-2b-86-19-de
08002b8619de	(4, .)	Pwd	Pwd

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>mab</b>	Enables MAC authentication bypass on a port.
	<b>mab eap</b>	Configures a port to use Extensible Authentication Protocol (EAP).
	<b>mab request format attribute 1</b>	Specifies the format of the MAC address in the User-Name attribute of MAB-generated Access-Request packets.
	<b>mab request format attribute 32</b>	Enables VLAN ID-based MAC authentication on a switch.

**mab request format attribute 32**

# mab request format attribute 32

Use the **mab request format attribute 32 vlan access-vlan** global configuration command to enable VLAN ID-based MAC authentication on a switch. Use the **no** form of this command to return to the default setting.

**mab request format attribute 32 vlan access-vlan**

**no mab request format attribute 32 vlan access-vlan**

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

**Defaults** VLAN-ID based MAC authentication is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.

Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

**Examples** This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Switch(config)# mab request format attribute 32 vlan access-vlan
```

Related Commands	Command	Description
	<a href="#">authentication event</a>	Sets the action for specific authentication events.
	<a href="#">authentication fallback</a>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<a href="#">authentication host-mode</a>	Sets the authorization manager mode on a port.
	<a href="#">authentication open</a>	Enables or disables open access on a port.
	<a href="#">authentication order</a>	Sets the order of authentication methods used on a port.
	<a href="#">authentication periodic</a>	Enable or disables reauthentication on a port.
	<a href="#">authentication port-control</a>	Enables manual control of the port authorization state.

Command	Description
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
<b>mab</b>	Enables MAC-based authentication on a port.
<b>mab eap</b>	Configures a port to use the Extensible Authentication Protocol (EAP)
<b>show authentication</b>	Displays information about authentication manager events on the switch.

**mac access-group**

# mac access-group

Use the **mac access-group** interface configuration command to apply a MAC access control list (ACL) to a Layer 2 interface. Use the **no** form of this command to remove all MAC ACLs or the specified MAC ACL from the interface. You create the MAC ACL by using the **mac access-list extended** global configuration command.

```
mac access-group {name} in
no mac access-group {name}
```

<b>Syntax Description</b>	<table border="0"> <tr> <td><b>name</b></td><td>Specify a named MAC access list.</td></tr> <tr> <td><b>in</b></td><td>Specify that the ACL is applied in the ingress direction. Outbound ACLs are not supported on Layer 2 interfaces.</td></tr> </table>	<b>name</b>	Specify a named MAC access list.	<b>in</b>	Specify that the ACL is applied in the ingress direction. Outbound ACLs are not supported on Layer 2 interfaces.
<b>name</b>	Specify a named MAC access list.				
<b>in</b>	Specify that the ACL is applied in the ingress direction. Outbound ACLs are not supported on Layer 2 interfaces.				

**Defaults** No MAC ACL is applied to the interface.

**Command Modes** Interface configuration (Layer 2 interfaces only)

**Command History**

**Usage Guidelines** You can apply MAC ACLs only to ingress Layer 2 interfaces.

On Layer 2 interfaces, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC access lists. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP ACL and a MAC ACL to the interface. You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface.

If a MAC ACL is already configured on a Layer 2 interface and you apply a new MAC ACL to the interface, the new ACL replaces the previously configured one.

When an inbound packet is received on an interface with a MAC ACL applied, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards or drops the packet, according to the ACL.

If the specified ACL does not exist, the switch forwards all packets.

For more information about configuring MAC extended ACLs, see the “Configuring Network Security with ACLs” chapter in the software configuration guide for this release.

**Examples**

This example shows how to apply a MAC extended ACL named *macacl2* to an interface:

```
Switch(config-if)# mac access-group macacl2 in
```

You can verify your settings by entering the **show mac access-group** privileged EXEC command. You can see configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

**Related Commands**

Command	Description
<b>show access-lists</b>	Displays the ACLs configured on the switch.
<b>show link state group</b>	Displays the MAC ACLs configured on the switch.
<b>show running-config</b>	Displays the running configuration on the switch.

**mac access-list extended**

# mac access-list extended

Use the **mac access-list extended** global configuration command to create an access list based on MAC addresses for non-IP traffic. Using this command puts you in the extended MAC access-list configuration mode. Use the **no** form of this command to return to the default setting.

**mac access-list extended name**

**no mac access-list extended name**

<b>Syntax Description</b>	<b>name</b> Assign a name to the MAC extended access list.
<b>Defaults</b>	By default, there are no MAC access lists created.
<b>Command Modes</b>	Global configuration
<b>Command History</b>	
<b>Usage Guidelines</b>	<p>MAC named extended lists are used with class maps.</p> <p>You can apply named MAC extended ACLs to Layer 2 interfaces.</p> <p>Entering the <b>mac access-list extended</b> command enables the MAC access-list configuration mode. These configuration commands are available:</p> <ul style="list-style-type: none"> <li>• <b>default</b>: sets a command to its default.</li> <li>• <b>deny</b>: specifies packets to reject. For more information, see the <a href="#">deny (MAC access-list configuration)</a> MAC access-list configuration command.</li> <li>• <b>exit</b>: exits from MAC access-list configuration mode.</li> <li>• <b>no</b>: negates a command or sets its defaults.</li> <li>• <b>permit</b>: specifies packets to forward. For more information, see the <a href="#">permit (MAC access-list configuration)</a> command.</li> </ul> <p>For more information about MAC extended access lists, see the software configuration guide for this release.</p>
<b>Examples</b>	<p>This example shows how to create a MAC named extended access list named <i>mac1</i> and to enter extended MAC access-list configuration mode:</p> <pre>Switch(config)# mac access-list extended mac1 Switch(config-ext-mac1) #</pre> <p>This example shows how to delete MAC named extended access list <i>mac1</i>:</p> <pre>Switch(config)# no mac access-list extended mac1</pre> <p>You can verify your settings by entering the <b>show access-lists</b> privileged EXEC command.</p>

Related Commands	Command	Description
	<a href="#">deny (MAC access-list configuration)</a>	Configures the MAC ACL (in extended MAC-access list configuration mode).
	<a href="#">permit (MAC access-list configuration)</a>	
	<a href="#">show access-lists</a>	Displays the access lists configured on the switch.

---

 mac address-table aging-time

# mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to return to the default setting. The aging time applies to all VLANs or a specified VLAN.

**mac address-table aging-time {0 | 10-1000000} [vlan vlan-id]**

**no mac address-table aging-time {0 | 10-1000000} [vlan vlan-id]**

<b>Syntax Description</b>	<b>0</b> This value disables aging. Static address entries are never aged or removed from the table. <b>10-1000000</b> Aging time in seconds. The range is 10 to 1000000 seconds. <b>vlan vlan-id</b> (Optional) Specify the VLAN ID to which to apply the aging time. The range is 1 to 4094.
---------------------------	--

---

**Defaults** The default is 300 seconds.

---

**Command Modes** Global configuration

---

**Command History**

**Usage Guidelines** If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

If you do not specify a specific VLAN, this command sets the aging time for all VLANs.

---

**Examples** This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mac address-table aging-time</a>	Displays the MAC address table aging time for all VLANs or the specified VLAN.

# mac address-table learning vlan

Use the **mac address-table learning** global configuration command to enable MAC address learning on a VLAN. This is the default state. Use the **no** form of this command to disable MAC address learning on a VLAN to control which VLANs can learn MAC addresses.

**mac address-table learning vlan *vlan-id***

**no mac address-table learning vlan *vlan-id***

<b>Syntax Description</b>	<i>vlan-id</i>	Specify a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094.
---------------------------	----------------	---

**Defaults** By default, MAC address learning is enabled on all VLANs.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(46)SE1	This command was introduced.

**Usage Guidelines** When you control MAC address learning on a VLAN, you can manage the available MAC address table space by controlling which VLANs, and therefore which ports, can learn MAC addresses.

You can disable MAC address learning on a single VLAN ID (for example, **no mac address-table learning vlan 223**) or on a range of VLAN IDs (for example, **no mac address-table learning vlan 1-20, 15.**)

Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network. For example, if you disable MAC address learning on a VLAN with a configured switch virtual interface (SVI), the switch floods all IP packets in the Layer 2 domain. If you disable MAC address learning on a VLAN that includes more than two ports, every packet entering the switch is flooded in that VLAN domain. We recommend that you disable MAC address learning only in VLANs that contain two ports and that you use caution before disabling MAC address learning on a VLAN with an SVI.

You cannot disable MAC address learning on a VLAN that the switch uses internally. If the VLAN ID that you enter in the **no mac address-table learning vlan *vlan-id*** command is an internal VLAN, the switch generates an error message and rejects the command. To view used internal VLANs, enter the **show vlan internal usage** privileged EXEC command.

If you disable MAC address learning on a VLAN configured as a private VLAN primary or a secondary VLAN, the MAC addresses are still learned on the other VLAN (primary or secondary) that belongs to the private VLAN.

You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

**mac address-table learning vlan**

If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on the secure port. If you later disable port security on the interface, the disabled MAC address learning state is enabled.

To display MAC address learning status of all VLANs or a specified VLAN, enter the **show mac-address-table learning [vlan *vlan-id*] command**.

**Examples**

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac address-table learning vlan 2003
```

To display MAC address learning status of all VLANs or a specified VLAN, enter the **show mac address-table learning [vlan *vlan-id*] command**.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show mac address-table learning</b></a>	Displays the MAC address learning status on all VLANs or on the specified VLAN.

# mac address-table move update

Use the **mac address-table move update** global configuration command to enable the MAC address-table move update feature. Use the **no** form of this command to return to the default setting.

**mac address-table move update {receive | transmit}**

**no mac address-table move update {receive | transmit}**

<b>Syntax Description</b>	<b>receive</b> Specify that the switch processes MAC address-table move update messages. <b>transmit</b> Specify that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.
---------------------------	--

**Command Modes**      Global configuration.

**Defaults**      By default, the MAC address-table move update feature is disabled.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SED	This command was introduced.

**Usage Guidelines**      The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic. You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

**Examples**      This example shows how to configure an access switch to send MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

You can verify your settings by entering the **show mac address-table move update** privileged EXEC command.

**mac address-table move update**

Related Commands	Command	Description
	<a href="#">clear mac address-table move update</a>	Clears the MAC address-table move update global counters.
	<a href="#">debug matm move update</a>	Debugs the MAC address-table move update message processing.
	<a href="#">show mac address-table move update</a>	Displays the MAC address-table move update information on the switch.

# mac address-table notification

Use the **mac address-table notification** global configuration command to enable the MAC address notification feature on the switch. Use the **no** form of this command to return to the default setting.

```
mac address-table notification {change [history-size value | interval value] | mac-move |
    threshold [[limit percentage] interval time]}
```

```
no mac address-table notification {change [history-size value | interval value] | mac-move |
    threshold [[limit percentage] interval time]}
```

Syntax Description	
<b>change</b>	Enable or disable the MAC notification on the switch.
<b>history-size</b> <i>value</i>	(Optional) Configure the maximum number of entries in the MAC notification history table. The range is 0 to 500 entries. The default is 1.
<b>interval</b> <i>value</i>	(Optional) Set the notification trap interval. The switch sends the notification traps when this amount of time has elapsed. The range is 0 to 2147483647 seconds. The default is 1 second.
<b>mac-move</b>	Enable MAC move notification.
<b>threshold</b>	Enable MAC threshold notification.
<b>limit</b> <i>percentage</i>	(Optional) Enter the MAC utilization threshold percentage. The range is 1 to 100 percent. The default is 50 percent.
<b>interval</b> <i>time</i>	(Optional) Enter the time between MAC threshold notifications. The range is 120 to 1000000 seconds. The default is 120 seconds.

## Defaults

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled. The default MAC change trap interval is 1 second. The default number of entries in the history table is 1. The default MAC utilization threshold is 50 percent. The default time between MAC threshold notifications is 120 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(40)SE	The <b>change</b> , <b>mac-move</b> , and <b>threshold</b> [[ <b>limit percentage</b> ] <b>interval time</b> ] keywords were added.

## Usage Guidelines

The MAC address notification change feature sends Simple Network Management Protocol (SNMP) traps to the network management system (NMS) whenever a new MAC address is added or an old address is deleted from the forwarding tables. MAC change notifications are generated only for dynamic and secure MAC addresses and are not generated for self addresses, multicast addresses, or other static addresses.

### mac address-table notification

When you configure the **history-size** option, the existing MAC address history table is deleted, and a new table is created.

You enable the MAC address notification change feature by using the **mac address-table notification change** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification change** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification change** global configuration command.

You can also enable traps whenever a MAC address is moved from one port to another in the same VLAN by entering the **mac address-table notification mac-move** command and the **snmp-server enable traps mac-notification move** global configuration command.

To generate traps whenever the MAC address table threshold limit is reached or exceeded, enter the **mac address-table notification threshold [limit percentage] | [interval time]** command and the **snmp-server enable traps mac-notification threshold** global configuration command.

### Examples

This example shows how to enable the MAC address-table change notification feature, set the interval time to 60 seconds, and set the history-size to 100 entries:

```
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

### Related Commands

Command	Description
<a href="#">clear mac address-table notification</a>	Clears the MAC address notification global counters.
<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings on all interfaces or on the specified interface.
<a href="#">snmp-server enable traps</a>	Sends the SNMP MAC notification traps when the <b>mac-notification</b> keyword is appended.
<a href="#">snmp trap mac-notification change</a>	Enables the SNMP MAC notification change trap on a specific interface.

# mac address-table static

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the table.

**mac address-table static *mac-addr* *vlan* *vlan-id* *interface* *interface-id***

**no mac address-table static *mac-addr* *vlan* *vlan-id* [*interface* *interface-id*]**

Syntax Description	<i>mac-addr</i>	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
	<b>vlan</b> <i>vlan-id</i>	Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
	<b>interface</b> <i>interface-id</i>	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

**Defaults** No static addresses are configured.

**Command Modes** Global configuration

## Command History

### Examples

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

### Related Commands

Command	Description
<b>show mac address-table static</b>	Displays static MAC address table entries only.

**mac address-table static drop**

# mac address-table static drop

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the **no** form of this command to return to the default setting.

**mac address-table static mac-addr vlan vlan-id drop**

**no mac address-table static mac-addr vlan vlan-id**

<b>Syntax Description</b>	<p><b>mac-addr</b> Unicast source or destination MAC address. Packets with this MAC address are dropped.</p> <p><b>vlan vlan-id</b> Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.</p>
---------------------------	---

**Defaults** Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the **mac address-table static mac-addr vlan vlan-id interface interface-id** global configuration command followed by the **mac address-table static mac-addr vlan vlan-id drop** command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the **mac address-table static mac-addr vlan vlan-id drop** global configuration command followed by the **mac address-table static mac-addr vlan vlan-id interface interface-id** command, the switch adds the MAC address as a static address.

### Examples

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

This example shows how to disable unicast MAC address filtering:

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

You can verify your setting by entering the **show mac address-table static** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show mac address-table static</a>	Displays only static MAC address table entries.

**match (class-map configuration)**

# match (class-map configuration)

Use the **match** class-map configuration command to define the match criteria to classify traffic. Use the **no** form of this command to remove the match criteria.

```
match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list}
no match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list}
```

Syntax Description	access-group <i>acl-index-or-name</i>	Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
	<b>ip dscp</b> <i>dscp-list</i>	List of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly-used value.
	<b>ip precedence</b> <i>ip-precedence-list</i>	List of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly-used value

**Defaults**

No match criteria are defined.

**Command Modes**

Class-map configuration

**Command History****Usage Guidelines**

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access-group matching to the Ether Type/Len are supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-all** and **match-any** keywords are equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

**Examples**

This example shows how to create a class map called *class2*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

This example shows how to create a class map called *class3*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using *ac11*:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group ac11
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
<a href="#">show class-map</a>	Displays quality of service (QoS) class maps.

**mdix auto**

# mdix auto

Use the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the **no** form of this command to disable auto-MDIX.

**mdix auto**

**no mdix auto**

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

**Defaults** Auto-MDIX is enabled.

**Command Modes** Interface configuration

## Command History

**Usage Guidelines** When you enable auto-MDIX on an interface, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed and duplex) is enabled on one or both of connected interfaces, link up occurs, even if the cable type (straight-through or crossover) is incorrect.

## Examples

This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller interface-id phy** privileged EXEC command.

# mls qos

Use the **mls qos** global configuration command to enable quality of service (QoS) for the entire switch. When the **mls qos** command is entered, QoS is enabled with the default parameters on all ports in the system. Use the **no** form of this command to reset all the QoS-related statistics and to disable the QoS features for the entire switch.

**mls qos**

**no mls qos**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

## Defaults

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

When QoS is enabled with the **mls qos** global configuration command and all other QoS settings are set to their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted. The default ingress and egress queue settings are in effect.

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

## Command History

### Usage Guidelines

QoS must be globally enabled to use QoS classification, policing, mark down or drop, queueing, and traffic shaping features. You can create a policy-map and attach it to a port before entering the **mls qos** command. However, until you enter the **mls qos** command, QoS processing is disabled.

Policy-maps and class-maps used to configure QoS are not deleted from the configuration by the **no mls qos** command, but entries corresponding to policy maps are removed from the switch hardware to save system resources. To re-enable QoS with the previous configurations, use the **mls qos** command.

Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets for this queue.

<b>Examples</b>	This example shows how to enable QoS on the switch:
-----------------	---

```
Switch(config)# mls qos
```

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

## Related Commands

**mls qos**

Command	Description
<b>show mls qos</b>	Displays QoS information.

# mls qos aggregate-policer

Use the **mls qos aggregate-policer** global configuration command to define policer parameters, which can be shared by multiple classes within the same policy map. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. Use the **no** form of this command to delete an aggregate policer.

```
mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action {drop | policed-dscp-transmit}
```

```
no mls qos aggregate-policer aggregate-policer-name
```

Syntax Description		
	<i>aggregate-policer-name</i>	Name of the aggregate policer referenced by the <b>police aggregate</b> policy-map class configuration command.
	<i>rate-bps</i>	Specify the average traffic rate in bits per second (b/s). The range is 8000 to 1000000000.
	<i>burst-byte</i>	Specify the normal burst size in bytes. The range is 8000 to 1000000.
	<b>exceed-action drop</b>	When the specified rate is exceeded, specify that the switch drop the packet.
	<b>exceed-action policed-dscp-transmit</b>	When the specified rate is exceeded, specify that the switch change the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then send the packet.

**Defaults** No aggregate policers are defined.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

Define an aggregate policer if the policer is shared with multiple classes.

Policers for a port cannot be shared with other policers for another port; traffic from two different ports cannot be aggregated for policing purposes.

The port ASIC device, which controls more than one physical port, supports 256 policers (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of user-configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port (there is no guarantee that a port will be assigned to any policer).

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.

You cannot delete an aggregate policer if it is being used in a policy map. You must first use the **no police aggregate** *aggregate-policer-name* policy-map class configuration command to delete the aggregate policer from all policy maps before using the **no mls qos aggregate-policer** *aggregate-policer-name* command.

**■ mls qos aggregate-policer**

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

**Examples**

This example shows how to define the aggregate policer parameters and how to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 1000000 1000000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">police aggregate</a>	Creates a policer that is shared by different classes.
<a href="#">show mls qos aggregate-policer</a>	Displays the quality of service (QoS) aggregate policer configuration.

## mls qos cos

Use the **mls qos cos** interface configuration command to define the default class of service (CoS) value of a port or to assign the default CoS to all incoming packets on the port. Use the **no** form of this command to return to the default setting.

**mls qos cos {default-cos | override}**

**no mls qos cos {default-cos | override}**

<b>Syntax Description</b>	<b>default-cos</b> Assign a default CoS value to a port. If packets are untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7. <b>override</b> Override the CoS of the incoming packets, and apply the default CoS value on the port to all incoming packets.
---------------------------	--

<b>Defaults</b>	The default CoS value for a port is 0. CoS override is disabled.
-----------------	---

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

### Command History

<b>Usage Guidelines</b>	You can use the default value to assign a CoS and Differentiated Services Code Point (DSCP) value to all incoming packets that are untagged (if the incoming packet does not have a CoS value). You also can assign a default CoS and DSCP value to all incoming packets by using the <b>override</b> keyword.
-------------------------	--

Use the **override** keyword when all incoming packets on certain ports deserve higher or lower priority than packets entering from other ports. Even if a port is previously set to trust DSCP, CoS, or IP precedence, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

<b>Examples</b>	This example shows how to configure the default port CoS to 4 on a port:
-----------------	--

```
Switch(config)# interface
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

**■ mls qos cos**

This example shows how to assign all the packets entering a port to the default port CoS value of 4 on a port:

```
Switch(config)# interface
Switch(config-if)# mls qos cos 4
Switch(config-if)# mls qos cos override
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">show mls qos interface</a>	Displays quality of service (QoS) information.

# mls qos dscp-mutation

Use the **mls qos dscp-mutation** interface configuration command to apply a Differentiated Services Code Point (DSCP)-to-DSCP-mutation map to a DSCP-trusted port. Use the **no** form of this command to return the map to the default settings (no DSCP mutation).

**mls qos dscp-mutation *dscp-mutation-name***

**no mls qos dscp-mutation *dscp-mutation-name***

<b>Syntax Description</b>	<i>dscp-mutation-name</i>	Name of the DSCP-to-DSCP-mutation map. This map was previously defined with the <b>mls qos map dscp-mutation</b> global configuration command.
---------------------------	---------------------------	--

<b>Defaults</b>	The default DSCP-to-DSCP-mutation map is a null map, which maps incoming DSCPs to the same DSCP values.
-----------------	---

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

## Command History

### Usage Guidelines

If two quality of service (QoS) domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a quality of service (QoS) administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS handles the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on ingress ports.

You apply the map only to DSCP-trusted ports. If you apply the DSCP mutation map to an untrusted port, to class of service (CoS) or IP-precedence trusted port, the command has no immediate effect until the port becomes DSCP-trusted.

### Examples

This example shows how to define the DSCP-to-DSCP-mutation map named *dscpmutation1* and to apply the map to a port:

```
Switch(config)# mls qos map dscp-mutation dscpmutation1 10 11 12 13 to 30
Switch(config)# interface
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

This example show how to remove the DSCP-to-DSCP-mutation map name *dscpmutation1* from the port and to reset the map to the default:

```
Switch(config-if)# no mls qos dscp-mutation dscpmutation1
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

**■ mls qos dscp-mutation**

Related Commands	Command	Description
	<b>mls qos map dscp-mutation</b>	Defines the DSCP-to-DSCP-mutation map.
	<b>mls qos trust</b>	Configures the port trust state.
	<b>show mls qos maps</b>	Displays QoS mapping information.

## mls qos map

Use the **mls qos map** global configuration command to define the class of service (CoS)-to-Differentiated Services Code Point (DSCP) map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map. Use the **no** form of this command to return to the default map.

```
mls qos map {cos-dscp dscp1...dscp8 | dscp-cos dscp-list to cos | dscp-mutation
dscp-mutation-name in-dscp to out-dscp | ip-prec-dscp dscp1...dscp8 | policed-dscp dscp-list
to mark-down-dscp}
```

```
no mls qos map {cos-dscp | dscp-cos | dscp-mutation dscp-mutation-name | ip-prec-dscp |
policed-dscp}
```

Syntax Description	cos-dscp <i>dscp1...dscp8</i>	Define the CoS-to-DSCP map. For <i>dscp1...dscp8</i> , enter eight DSCP values that correspond to CoS values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63.
<b>dscp-cos <i>dscp-list to cos</i></b>	<b>dscp-cos <i>dscp-list to cos</i></b>	Define the DSCP-to-CoS map. For <i>dscp-list</i> , enter up to eight DSCP values, with each value separated by a space. The range is 0 to 63. Then enter the <b>to</b> keyword. For <i>cos</i> , enter a single CoS value to which the DSCP values correspond. The range is 0 to 7.
<b>dscp-mutation</b>	<b>dscp-mutation</b>	Define the DSCP-to-DSCP-mutation map. For <i>dscp-mutation-name</i> , enter the mutation map name.
<i>dscp-mutation-name in-dscp to out-dscp</i>	<i>dscp-mutation-name in-dscp to out-dscp</i>	For <i>in-dscp</i> , enter up to eight DSCP values, with each value separated by a space. Then enter the <b>to</b> keyword. For <i>out-dscp</i> , enter a single DSCP value. The range is 0 to 63.
<b>ip-prec-dscp</b>	<b>ip-prec-dscp</b>	Define the IP-precedence-to-DSCP map. For <i>dscp1...dscp8</i> , enter eight DSCP values that correspond to the IP precedence values 0 to 7. Separate each DSCP value with a space. The range is 0 to 63.
<b>policed-dscp <i>dscp-list to mark-down-dscp</i></b>	<b>policed-dscp <i>dscp-list to mark-down-dscp</i></b>	Define the policed-DSCP map. For <i>dscp-list</i> , enter up to eight DSCP values, with each value separated by a space. Then enter the <b>to</b> keyword. For <i>mark-down-dscp</i> , enter the corresponding policed (marked down) DSCP value. The range is 0 to 63.

**mls qos map****Defaults**

Table 2-14 shows the default CoS-to-DSCP map:

**Table 1-14 Default CoS-to-DSCP Map**

<b>CoS Value</b>	<b>DSCP Value</b>
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Table 2-15 shows the default DSCP-to-CoS map:

**Table 1-15 Default DSCP-to-CoS Map**

<b>DSCP Value</b>	<b>CoS Value</b>
0–7	0
8–15	1
16–23	2
24–31	3
32–39	4
40–47	5
48–55	6
56–63	7

Table 2-16 shows the default IP-precedence-to-DSCP map:

**Table 1-16 Default IP-Precedence-to-DSCP Map**

<b>IP Precedence Value</b>	<b>DSCP Value</b>
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

All the maps are globally defined. All the maps, except the DSCP-to-DSCP-mutation map, are applied to all ports. The DSCP-to-DSCP-mutation map is applied to a specific port.

## Examples

This example shows how to define the IP-precedence-to-DSCP map and to map IP-precedence values 0 to 7 to DSCP values of 0, 10, 20, 30, 40, 50, 55, and 60:

```
Switch# configure terminal
Switch(config)# mls qos map ip-prec-dscp 0 10 20 30 40 50 55 60
```

This example shows how to define the policed-DSCP map. DSCP values 1, 2, 3, 4, 5, and 6 are marked down to DSCP value 0. Marked DSCP values that not explicitly configured are not modified:

```
Switch# configure terminal
Switch(config)# mls qos map policed-dscp 1 2 3 4 5 6 to 0
```

This example shows how to define the DSCP-to-CoS map. DSCP values 20, 21, 22, 23, and 24 are mapped to CoS 1. DSCP values 10, 11, 12, 13, 14, 15, 16, and 17 are mapped to CoS 0:

```
Switch# configure terminal
Switch(config)# mls qos map dscp-cos 20 21 22 23 24 to 1
Switch(config)# mls qos map dscp-cos 10 11 12 13 14 15 16 17 to 0
```

This example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 0, 5, 10, 15, 20, 25, 30, and 35:

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 0 5 10 15 20 25 30 35
```

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remain as specified in the null map):

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 10
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 0 31 32 33 34 to 30
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

**■ mls qos map****Related Commands**

Command	Description
<a href="#">mls qos dscp-mutation</a>	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
<a href="#">show mls qos maps</a>	Displays quality of service (QoS) mapping information.

# mls qos queue-set output buffers

Use the **mls qos queue-set output buffers** global configuration command to allocate buffers to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

**mls qos queue-set output *qset-id* buffers *allocation1* ... *allocation4***

**no mls qos queue-set output *qset-id* buffers**

<b>Syntax Description</b>	<p><i>qset-id</i> ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.</p> <p><i>allocation1</i> ... <i>allocation4</i> Buffer space allocation (percentage) for each queue (four values for queues 1 to 4). For <i>allocation1</i>, <i>allocation3</i>, and <i>allocation4</i>, the range is 0 to 99. For <i>allocation2</i>, the range is 1 to 100 (including the CPU buffer). Separate each value with a space.</p>
---------------------------	---

<b>Defaults</b>	All allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 of the buffer space.
-----------------	--

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

## Command History

### Usage Guidelines

Specify four allocation values, and separate each with a space.

Allocate buffers according to the importance of the traffic; for example, give a large percentage of the buffer to the queue with the highest-priority traffic.

To configure different classes of traffic with different characteristics, use this command with the **mls qos queue-set output *qset-id* threshold** global configuration command.



### Note

The egress queue default settings are suitable for most situations. Change them only when you have a thorough understanding of the egress queues. For information about QoS, see the “Configuring QoS” chapter in the software configuration guide.

**mls qos queue-set output buffers****Examples**

This example shows how to map a port to queue-set 2. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent to egress queues 2, 3, and 4:

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# interface
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** or the **show mls qos queue-set** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>mls qos queue-set output threshold</b></a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<a href="#"><b>queue-set</b></a>	Maps a port to a queue-set.
<a href="#"><b>show mls qos interface buffers</b></a>	Displays quality of service (QoS) information.
<a href="#"><b>show mls qos queue-set</b></a>	Displays egress queue settings for the queue-set.

# mls qos queue-set output threshold

Use the **mls qos queue-set output threshold** global configuration command to configure the weighted tail-drop (WTD) thresholds, to guarantee the availability of buffers, and to configure the maximum memory allocation to a queue-set (four egress queues per port). Use the **no** form of this command to return to the default setting.

**mls qos queue-set output *qset-id* threshold *queue-id* drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold**

**no mls qos queue-set output *qset-id* threshold [*queue-id*]**

## Syntax Description

<i>qset-id</i>	ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
<i>queue-id</i>	Specific queue in the queue-set on which the command is performed. The range is 1 to 4.
<i>drop-threshold1</i> <i>drop-threshold2</i>	Two WTD thresholds expressed as a percentage of the allocated memory of the queue. The range is 1 to 3200 percent.
<i>reserved-threshold</i>	Amount of memory to be guaranteed (reserved) for the queue and expressed as a percentage of the allocated memory. The range is 1 to 100 percent.
<i>maximum-threshold</i>	Enable a queue in the full condition to get more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped. The range is 1 to 3200 percent.

## Defaults

When quality of service (QoS) is enabled, WTD is enabled.

[Table 2-17](#) shows the default WTD threshold settings.

**Table 1-17 Default Egress Queue WTD Threshold Settings**

Feature	Queue 1	Queue 2	Queue 3	Queue 4
WTD drop threshold 1	100 percent	200 percent	100 percent	100 percent
WTD drop threshold 2	100 percent	200 percent	100 percent	100 percent
Reserved threshold	50 percent	100 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent

## Command Modes

Global configuration

## Command History

### Usage Guidelines

Use the **mls qos queue-set output *qset-id* buffers** global configuration command to allocate a fixed number of buffers to the four queues in a queue-set.

The drop-threshold percentages can exceed 100 percent and can be up to the maximum (if the maximum threshold exceeds 100 percent).

**mls qos queue-set output threshold**

While buffer ranges allow individual queues in the queue-set to use more of the common pool when available, the maximum number of packets for each queue is still internally limited to 400 percent, or 4 times the allocated number of buffers. One packet can use one 1 or more buffers.

The range increased in Cisco IOS Release 12.2(25)SEE1 or later for the *drop-threshold*, *drop-threshold2*, and *maximum-threshold* parameters.



**Note** The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to decide whether to grant buffer space to a requesting queue. The switch decides whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over-limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

**Examples**

This example shows how to map a port to queue-set 2. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory this queue can have before packets are dropped:

```
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** or the **show mls qos queue-set** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
<a href="#">queue-set</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface buffers</a>	Displays QoS information.
<a href="#">show mls qos queue-set</a>	Displays egress queue settings for the queue-set.

# mls qos rewrite ip dscp

Use the **mls qos rewrite ip dscp** global configuration command to configure the switch to change (rewrite) the Differentiated Services Code Point (DSCP) field of an incoming IP packet. Use the **no** form of this command to configure the switch to not modify (rewrite) the DSCP field of the packet and to enable DSCP transparency.

**mls qos rewrite ip dscp**

**no mls qos rewrite ip dscp**

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

**Defaults** DSCP transparency is disabled. The switch changes the DSCP field of the incoming IP packet.

**Command Modes** Global configuration

## Command History

## Usage Guidelines

DSCP transparency affects only the DSCP field of a packet at the egress. If DSCP transparency is enabled by using the **no mls qos rewrite ip dscp** command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.

By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing and marking, and the DSCP-to-DSCP mutation map.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet that the switch uses to generate a class of service (CoS) value representing the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

For example, if QoS is enabled and an incoming packet has a DSCP value of 32, the switch might modify the internal DSCP value based on the policy-map configuration and change the internal DSCP value to 16. If DSCP transparency is enabled, the outgoing DSCP value is 32 (same as the incoming value). If DSCP transparency is disabled, the outgoing DSCP value is 16 because it is based on the internal DSCP value.

---

■ **mls qos rewrite ip dscp**

**Examples**

This example shows how to enable DSCP transparency and configure the switch to not change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# no mls qos rewrite ip dscp
```

This example shows how to disable DSCP transparency and configure the switch to change the DSCP value of the incoming IP packet:

```
Switch(config)# mls qos
Switch(config)# mls qos rewrite ip dscp
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>mls qos</b></a>	Enables QoS globally.
<a href="#"><b>show mls qos</b></a>	Displays QoS information.
<a href="#"><b>show running-config   include rewrite</b></a>	Displays the DSCP transparency setting.

# mls qos srr-queue input bandwidth

Use the **mls qos srr-queue input bandwidth** global configuration command to assign shaped round robin (SRR) weights to an ingress queue. The ratio of the weights is the ratio of the frequency in which the SRR scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

```
mls qos srr-queue input bandwidth weight1 weight2
no mls qos srr-queue input bandwidth
```

<b>Syntax Description</b>	<i>weight1 weight2</i>	Ratio of <i>weight1</i> and <i>weight2</i> determines the ratio of the frequency in which the SRR scheduler dequeues packets from ingress queues 1 and 2. The range is 1 to 100. Separate each value with a space.
---------------------------	------------------------	--

**Defaults** Weight1 and weight2 are 4 (1/2 of the bandwidth is equally shared between the two queues).

**Command Modes** Global configuration

## Command History

**Usage Guidelines** SRR services the priority queue for its configured weight as specified by the **bandwidth** keyword in the **mls qos srr-queue input priority-queue queue-id bandwidth weight** global configuration command. Then SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the **mls qos srr-queue input bandwidth weight1 weight2** global configuration command.

You specify which ingress queue is the priority queue by using the **mls qos srr-queue input priority-queue** global configuration command.

## Examples

This example shows how to assign the ingress bandwidth for the queues. Priority queueing is disabled, and the shared bandwidth ratio allocated to queue 1 is 25/(25+75) and to queue 2 is 75/(25+75):

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

In this example, queue 2 has three times the bandwidth of queue 1; queue 2 is serviced three times as often as queue 1.

This example shows how to assign the ingress bandwidths for the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratio allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue:

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

### **■ mls qos srr-queue input bandwidth**

You can verify your settings by entering the **show mls qos interface [interface-id] queueing** or the **show mls qos input-queue** privileged EXEC command.

#### **Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>mls qos srr-queue input buffers</b></a>	Allocates the buffers between the ingress queues.
<a href="#"><b>mls qos srr-queue input cos-map</b></a>	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<a href="#"><b>mls qos srr-queue input dscp-map</b></a>	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#"><b>mls qos srr-queue input priority-queue</b></a>	Configures the ingress priority queue and guarantees bandwidth.
<a href="#"><b>mls qos srr-queue input threshold</b></a>	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.
<a href="#"><b>show mls qos input-queue</b></a>	Displays ingress queue settings.
<a href="#"><b>show mls qos interface queueing</b></a>	Displays quality of service (QoS) information.

# mls qos srr-queue input buffers

Use the **mls qos srr-queue input buffers** global configuration command to allocate the buffers between the ingress queues. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue input buffers *percentage1 percentage2***

**no mls qos srr-queue input buffers**

<b>Syntax Description</b>	<i>percentage1</i> Percentage of buffers allocated to ingress queues 1 and 2. The range is 0 to 100. Separate each value with a space. <i>percentage2</i>
---------------------------	--

**Defaults** Ninety percent of the buffers is allocated to queue 1, and 10 percent of the buffers is allocated to queue 2.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** You should allocate the buffers so that the queues can handle any incoming bursty traffic.

**Examples** This example shows how to allocate 60 percent of the buffer space to ingress queue 1 and 40 percent of the buffer space to ingress queue 2:

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** or the **show mls qos input-queue** privileged EXEC command.

■ **mls qos srr-queue input buffers**

Related Commands	Command	Description
	<b>mls qos srr-queue input bandwidth</b>	Assigns shaped round robin (SRR) weights to an ingress queue.
	<b>mls qos srr-queue input cos-map</b>	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
	<b>mls qos srr-queue input dscp-map</b>	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
	<b>mls qos srr-queue input priority-queue</b>	Configures the ingress priority queue and guarantees bandwidth.
	<b>mls qos srr-queue input threshold</b>	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.
	<b>show mls qos input-queue</b>	Displays ingress queue settings.
	<b>show mls qos interface buffers</b>	Displays quality of service (QoS) information.

# mls qos srr-queue input cos-map

Use the **mls qos srr-queue input cos-map** global configuration command to map class of service (CoS) values to an ingress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue input cos-map queue *queue-id* {cos1...cos8 | threshold *threshold-id* cos1...cos8}**

**no mls qos srr-queue input cos-map**

<b>Syntax Description</b>	<b>queue <i>queue-id</i></b> Specify a queue number. For <i>queue-id</i> , the range is 1 to 2.
<b>cos1...cos8</b>	Map CoS values to an ingress queue.  For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.
<b>threshold <i>threshold-id</i></b> <b>cos1...cos8</b>	Map CoS values to a queue threshold ID.  For <i>threshold-id</i> , the range is 1 to 3.  For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.

## Defaults

Table 2-18 shows the default CoS input queue threshold map:

**Table 2-18 Default CoS Input Queue Threshold Map**

CoS Value	Queue ID - Threshold ID
0–4	1–1
5	2–1
6, 7	1–1

## Command Modes

Global configuration

## Command History

### Usage Guidelines

The CoS assigned at the ingress port selects an ingress or egress queue and threshold.

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. You can assign two weighted tail-drop (WTD) threshold percentages to an ingress queue by using the **mls qos srr-queue input threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

---

```
■ mls qos srr-queue input cos-map
```

**Examples**

This example shows how to map CoS values 0 to 3 to ingress queue 1 and to threshold ID 1 with a drop threshold of 50 percent. It maps CoS values 4 and 5 to ingress queue 1 and to threshold ID 2 with a drop threshold of 70 percent:

```
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos srr-queue input cos-map queue 1 threshold 2 4 5
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">mls qos srr-queue input bandwidth</a>	Assigns shaped round robin (SRR) weights to an ingress queue.
<a href="#">mls qos srr-queue input buffers</a>	Allocates the buffers between the ingress queues.
<a href="#">mls qos srr-queue input dscp-map</a>	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue input priority-queue</a>	Configures the ingress priority queue and guarantees bandwidth.
<a href="#">mls qos srr-queue input threshold</a>	Assigns WTD threshold percentages to an ingress queue.
<a href="#">show mls qos maps</a>	Displays QoS mapping information.

# mls qos srr-queue input dscp-map

Use the **mls qos srr-queue input dscp-map** global configuration command to map Differentiated Services Code Point (DSCP) values to an ingress queue or to map DSCP values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue input dscp-map queue *queue-id* {*dscp1...dscp8* | threshold *threshold-id* *dscp1...dscp8*}**

**no mls qos srr-queue input dscp-map**

## Syntax Description

<b>queue <i>queue-id</i></b>	Specify a queue number. For <i>queue-id</i> , the range is 1 to 2.
<b><i>dscp1...dscp8</i></b>	Map DSCP values to an ingress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.
<b>threshold <i>threshold-id</i></b>	Map DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.

## Defaults

Table 2-19 shows the default DSCP input queue threshold map:

**Table 2-19 Default DSCP Input Queue Threshold Map**

DSCP Value	Queue ID–Threshold ID
0–39	1–1
40–47	2–1
48–63	1–1

## Command Modes

Global configuration

## Command History

### Usage Guidelines

The DSCP assigned at the ingress port selects an ingress or egress queue and threshold.

The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state. You can assign two weighted tail-drop (WTD) threshold percentages to an ingress queue by using the **mls qos srr-queue input threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

---

```
■ mls qos srr-queue input dscp-map
```

**Examples**

This example shows how to map DSCP values 0 to 6 to ingress queue 1 and to threshold 1 with a drop threshold of 50 percent. It maps DSCP values 20 to 26 to ingress queue 1 and to threshold 2 with a drop threshold of 70 percent:

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

You can verify your settings by entering the **show mls qos maps** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">mls qos srr-queue input bandwidth</a>	Assigns shaped round robin (SRR) weights to an ingress queue.
<a href="#">mls qos srr-queue input buffers</a>	Allocates the buffers between the ingress queues.
<a href="#">mls qos srr-queue input cos-map</a>	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to threshold ID.
<a href="#">mls qos srr-queue input priority-queue</a>	Configures the ingress priority queue and guarantees bandwidth.
<a href="#">mls qos srr-queue input threshold</a>	Assigns WTD threshold percentages to an ingress queue.
<a href="#">show mls qos maps</a>	Displays QoS mapping information.

# mls qos srr-queue input priority-queue

Use the **mls qos srr-queue input priority-queue** global configuration command to configure the ingress priority queue and to guarantee bandwidth on the ring if the ring is congested. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue input priority-queue *queue-id bandwidth weight***

**no mls qos srr-queue input priority-queue *queue-id***

## Syntax Description

<b><i>queue-id</i></b>	Ingress queue ID. The range is 1 to 2.
<b>bandwidth <i>weight</i></b>	Bandwidth percentage of the ring. The range is 0 to 40.

## Defaults

The priority queue is queue 2, and 10 percent of the bandwidth is allocated to it.

## Command Modes

Global configuration

## Command History

## Usage Guidelines

You should use the priority queue only for traffic that needs to be expedited (for example, voice traffic, which needs minimum delay and jitter).

The priority queue is guaranteed part of the bandwidth on the ring, which reduces the delay and jitter under heavy network traffic on an oversubscribed (when there is more traffic than the backplane can carry, and the queues are full and dropping frames).

Shaped round robin (SRR) services the priority queue for its configured weight as specified by the **bandwidth** keyword in the **mls qos srr-queue input priority-queue *queue-id bandwidth weight*** global configuration command. Then SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the **mls qos srr-queue input bandwidth *weight1 weight2*** global configuration command.

To disable priority queueing, set the bandwidth weight to 0, for example, **mls qos srr-queue input priority-queue *queue-id bandwidth 0***.

---

■ **mls qos srr-queue input priority-queue**

**Examples**

This example shows how to assign the ingress bandwidths for the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratio allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue:

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

You can verify your settings by entering the **show mls qos interface [interface-id] queueing** or the **show mls qos input-queue** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>mls qos srr-queue input bandwidth</b>	Assigns shaped round robin (SRR) weights to an ingress queue.
<b>mls qos srr-queue input buffers</b>	Allocates the buffers between the ingress queues.
<b>mls qos srr-queue input cos-map</b>	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue input dscp-map</b>	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos srr-queue input threshold</b>	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.
<b>show mls qos input-queue</b>	Displays ingress queue settings.
<b>show mls qos interface queueing</b>	Displays quality of service (QoS) information.

# mls qos srr-queue input threshold

Use the **mls qos srr-queue input threshold** global configuration command to assign weighted tail-drop (WTD) threshold percentages to an ingress queue. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue input threshold *queue-id threshold-percentage1 threshold-percentage2***

**no mls qos srr-queue input threshold *queue-id***

Syntax Description	<i>queue-id</i>	ID of the ingress queue. The range is 1 to 2.
	<i>threshold-percentage1</i> <i>threshold-percentage2</i>	Two WTD threshold percentage values. Each threshold value is a percentage of the total number of queue descriptors allocated for the queue. Separate each value with a space. The range is 1 to 100.

**Defaults** When quality of service (QoS) is enabled, WTD is enabled.

The two WTD thresholds are set to 100 percent.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

QoS uses the CoS-to-threshold map or the DSCP-to-threshold map to decide which class of service (CoS) or Differentiated Services Code Points (DSCPs) values are mapped to threshold 1 and to threshold 2. If threshold 1 is exceeded, packets with CoS or DSCPs assigned to this threshold are dropped until the threshold is no longer exceeded. However, packets assigned to threshold 2 continue to be queued and sent as long as the second threshold is not exceeded.

Each queue has two configurable (explicit) drop threshold and one preset (implicit) drop threshold (full).

You configure the CoS-to-threshold map by using the **mls qos srr-queue input cos-map** global configuration command. You configure the DSCP-to-threshold map by using the **mls qos srr-queue input dscp-map** global configuration command.

### Examples

This example shows how to configure the tail-drop thresholds for the two queues. The queue 1 thresholds are 50 percent and 100 percent, and the queue 2 thresholds are 70 percent and 100 percent:

```
Switch(config)# mls qos srr-queue input threshold 1 50 100
Switch(config)# mls qos srr-queue input threshold 2 70 100
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** or the **show mls qos input-queue** privileged EXEC command.

### Related Commands

■ **mls qos srr-queue input threshold**

Command	Description
<b>mls qos srr-queue input bandwidth</b>	Assigns shaped round robin (SRR) weights to an ingress queue.
<b>mls qos srr-queue input buffers</b>	Allocates the buffers between the ingress queues.
<b>mls qos srr-queue input cos-map</b>	Maps class of service (CoS) values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue input dscp-map</b>	Maps Differentiated Services Code Point (DSCP) values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos srr-queue input priority-queue</b>	Configures the ingress priority queue and guarantees bandwidth.
<b>show mls qos input-queue</b>	Displays ingress queue settings.
<b>show mls qos interface buffers</b>	Displays quality of service (QoS) information.

# mls qos srr-queue output cos-map

Use the **mls qos srr-queue output cos-map** global configuration command to map class of service (CoS) values to an egress queue or to map CoS values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue output cos-map queue *queue-id* {cos1...cos8 | threshold *threshold-id*}  
cos1...cos8}**

**no mls qos srr-queue output cos-map**

## Syntax Description

<b>queue <i>queue-id</i></b>	Specify a queue number.  For <i>queue-id</i> , the range is 1 to 4.
<b>cos1...cos8</b>	Map CoS values to an egress queue.  For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.
<b>threshold <i>threshold-id</i></b>	Map CoS values to a queue threshold ID.  For <i>threshold-id</i> , the range is 1 to 3.  For <i>cos1...cos8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 7.

## Defaults

Table 2-20 shows the default CoS output queue threshold map:

**Table 2-20 Default Cos Output Queue Threshold Map**

CoS Value	Queue ID–Threshold ID
0, 1	2–1
2, 3	3–1
4	4–1
5	1–1
6, 7	4–1

## Command Modes

Global configuration

## Command History

### Usage Guidelines



The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.

**■ mls qos srr-queue output cos-map**

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output qset-id threshold** global configuration command.

You can map each CoS value to a different queue and threshold combination, allowing the frame to follow different behavior.

**Examples**

This example shows how to map a port to queue-set 1. It maps CoS values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface [interface-id] buffers**, or the **show mls qos queue-set** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>mls qos srr-queue output dscp-map</b>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos queue-set output threshold</b>	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<b>queue-set</b>	Maps a port to a queue-set.
<b>show mls qos interface buffers</b>	Displays QoS information.
<b>show mls qos maps</b>	Displays QoS mapping information.
<b>show mls qos queue-set</b>	Displays egress queue settings for the queue-set.

# mls qos srr-queue output dscp-map

Use the **mls qos srr-queue output dscp-map** global configuration command to map Differentiated Services Code Point (DSCP) values to an egress or to map DSCP values to a queue and to a threshold ID. Use the **no** form of this command to return to the default setting.

**mls qos srr-queue output dscp-map queue *queue-id* {*dscp1...dscp8* | threshold *threshold-id* *dscp1...dscp8*}**

**no mls qos srr-queue output dscp-map**

---

<b>Syntax Description</b>	<b>queue <i>queue-id</i></b>	Specify a queue number. For <i>queue-id</i> , the range is 1 to 4.
	<b><i>dscp1...dscp8</i></b>	Map DSCP values to an egress queue. For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.
	<b>threshold <i>threshold-id</i></b>	Map DSCP values to a queue threshold ID. For <i>threshold-id</i> , the range is 1 to 3.  For <i>dscp1...dscp8</i> , enter up to eight values, and separate each value with a space. The range is 0 to 63.

---

## Defaults

Table 2-21 shows the default DSCP output queue threshold map:

**Table 1-21 Default DSCP Output Queue Threshold Map**

DSCP Value	Queue ID–Threshold ID
0–15	2–1
16–31	3–1
32–39	4–1
40–47	1–1
48–63	4–1

## Command Modes

Global configuration

## Command History

## Usage Guidelines



The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

---

```
mls qos srr-queue output dscp-map
```

You can assign two weighted tail-drop (WTD) threshold percentages to an egress queue by using the **mls qos queue-set output qset-id threshold** global configuration command.

You can map each DSCP value to a different queue and threshold combination, allowing the frame to follow different behavior.

You can map up to eight DSCP values per command.

---

### Examples

This example shows how to map a port to queue-set 1. It maps DSCP values 0 to 3 to egress queue 1 and to threshold ID 1. It configures the drop thresholds for queue 1 to 50 and 70 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped.

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 1 0 1 2 3
Switch(config)# mls qos queue-set output 1 threshold 1 50 70 100 200
Switch(config)# interface
Switch(config-if)# queue-set 1
```

You can verify your settings by entering the **show mls qos maps**, the **show mls qos interface [interface-id] buffers**, or the **show mls qos queue-set** privileged EXEC command.

---

### Related Commands

Command	Description
<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
<a href="#">mls qos queue-set output threshold</a>	Configures the WTD thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<a href="#">queue-set</a>	Maps a port to a queue-set.
<a href="#">show mls qos interface buffers</a>	Displays quality of service (QoS) information.
<a href="#">show mls qos maps</a>	Displays QoS mapping information.
<a href="#">show mls qos queue-set</a>	Displays egress queue settings for the queue-set.

# mls qos trust

Use the **mls qos trust** interface configuration command to configure the port trust state. Ingress traffic can be trusted, and classification is performed by examining the packet Differentiated Services Code Point (DSCP), class of service (CoS), or IP-precedence field. Use the **no** form of this command to return a port to its untrusted state.

```
mls qos trust [cos | device cisco-phone | dscp | ip-precedence]
no mls qos trust [cos | device | dscp | ip-precedence]
```

Syntax Description	
<b>cos</b>	(Optional) Classify an ingress packet by using the packet CoS value. For an untagged packet, use the port default CoS value.
<b>device cisco-phone</b>	(Optional) Classify an ingress packet by trusting the CoS or DSCP value sent from the Cisco IP Phone (trusted boundary), depending on the trust setting.
<b>dscp</b>	(Optional) Classify an ingress packet by using the packet DSCP value (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the default port CoS value is used.
<b>ip-precedence</b>	(Optional) Classify an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS is used if the packet is tagged. For an untagged packet, the port default CoS value is used.

**Defaults** The port is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the domain. Use this command to specify whether the port is trusted and which fields of the packet to use to classify traffic.

When a port is configured with trust DSCP or trust IP precedence and the incoming packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to CoS-to-DSCP map) if the packet is an IP packet.

**■ mls qos trust**

The trusted boundary feature prevents security problems if users disconnect their PCs from networked Cisco IP Phones and connect them to the switch port to take advantage of trusted CoS or DSCP settings. You must globally enable the Cisco Discovery Protocol (CDP) on the switch and on the port connected to the IP phone. If the telephone is not detected, trusted boundary disables the trusted setting on the switch or routed port and prevents misuse of a high-priority queue.

If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the incoming packets are trusted. If you configure the **mls qos cos override** interface configuration command on the switch port connected to the IP phone, the switch overrides the CoS of the incoming voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

Classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]**) and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration.

**Examples**

This example shows how to configure a port to trust the IP precedence field in the incoming packet:

```
Switch(config)# interface
Switch(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP Phone connected on a port is a trusted device:

```
Switch(config)# interface
Switch(config-if)# mls qos trust device cisco-phone
```

You can verify your settings by entering the **show mls qos interface** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>mls qos cos</b></a>	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
<a href="#"><b>mls qos dscp-mutation</b></a>	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
<a href="#"><b>mls qos map</b></a>	Defines the CoS-to-DSCP map, DSCP-to-CoS map, the DSCP-to-DSCP-mutation map, the IP-precedence-to-DSCP map, and the policed-DSCP map.
<a href="#"><b>show mls qos interface</b></a>	Displays QoS information.

## monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source or destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, and to limit (filter) SPAN source traffic to specific VLANs. Use the **no** form of this command to remove the SPAN or RSPAN session or to remove source or destination interfaces or filters from the SPAN or RSPAN session. For destination interfaces, the encapsulation options are ignored with the **no** form of the command.

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

```
monitor session session_number filter vlan vlan-id [, | -]
```

```
monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

```
no monitor session {session_number | all | local | remote}
```

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

```
no monitor session session_number filter vlan vlan-id [, | -]
```

```
no monitor session session_number source {interface interface-id [, | -] [both | rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]} | {remote vlan vlan-id}
```

### Syntax Description

<b>session_number</b>	Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66.
<b>destination</b>	Specify the SPAN or RSPAN destination. A destination must be a physical port.
<b>interface</b> <i>interface-id</i>	Specify the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type 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 .
<b>encapsulation replicate</b>	(Optional) Specify that the destination interface replicates the source interface encapsulation method.  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.
<b>ingress</b>	(Optional) Enable ingress traffic forwarding.
<b>dot1q</b> <b>vlan</b> <i>vlan-id</i>	Accept incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
<b>untagged</b> <b>vlan</b> <i>vlan-id</i>	Accept incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.

**■ monitor session**

<b>vlan</b> <i>vlan-id</i>	When used with only the <b>ingress</b> keyword, set default VLAN for ingress traffic.
<b>remote vlan</b> <i>vlan-id</i>	Specify 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).
,	(Optional) Specify 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) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen.
<b>filter</b> <i>vlan</i> <i>vlan-id</i>	Specify 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.
<b>source</b>	Specify the SPAN or RSPAN source. A source can be a physical port, a port channel, or a VLAN.
<b>both, rx, tx</b>	(Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
<b>source vlan</b> <i>vlan-id</i>	Specify the SPAN source interface as a VLAN ID. The range is 1 to 4094.
<b>all, local, remote</b>	Specify <b>all</b> , <b>local</b> , or <b>remote</b> with the <b>no monitor session</b> command to clear all SPAN and RSPAN, all local SPAN, or all RSPAN sessions.

**Defaults**

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.

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****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 two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch.

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

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.

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 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.

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.

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.)

## Examples

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

```
Switch(config)# monitor session 1 source interface both
Switch(config)# monitor session 1 destination interface
```

**■ monitor session**

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

```
Switch(config)# no monitor session 2 destination
```

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 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
Switch(config)# monitor session 1 source interface port-channel 2 tx
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
```

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 encapsulation replicate 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 ingress untagged vlan 5
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>remote-span</b>	Configures an RSPAN VLAN in vlan configuration mode.
<b>show monitor</b>	Displays SPAN and RSPAN session information.
<b>show running-config</b>	Displays the current operating configuration.

# mvr (global configuration)

Use the **mvr** global configuration command without keywords to enable the multicast VLAN registration (MVR) feature on the switch. Use the command with keywords to set the MVR mode for a switch, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN. Use the **no** form of this command to return to the default settings.

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

## Syntax Description

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

## Defaults

MVR is disabled by default.

The default MVR mode is compatible mode.

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

The default group ip address count is 0.

The default query response time is 5 tenths of or one-half second.

The default multicast VLAN for MVR is VLAN 1.

**mvr (global configuration)**

**Command Modes** Global configuration

**Command History****Usage Guidelines**

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

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

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

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

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

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

MVR can coexist with IGMP snooping on a switch.

**Examples**

This example shows how to enable MVR:

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

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

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

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

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

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

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

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

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

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

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

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

**Related Commands**

Command	Description
<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
<a href="#">show mvr</a>	Displays MVR global parameters or port parameters.

Command	Description
<b>show mvr interface</b>	Displays the configured MVR interfaces with their type, status, and Immediate Leave configuration. Also displays all MVR groups of which the interface is a member.
<b>show mvr members</b>	Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive.

# mvr (interface configuration)

Use the **mvr** interface configuration command to configure a Layer 2 port as a multicast VLAN registration (MVR) receiver or source port, to set the Immediate Leave feature, and to statically assign a port to an IP multicast VLAN and IP address. Use the **no** form of this command to return to the default settings.

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

**no mvr [immediate | type {source | receiver}| vlan *vlan-id* group [*ip-address*]]**

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

## Defaults

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

The Immediate Leave feature is disabled on all ports.

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

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

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

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

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

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

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

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

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

## Examples

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

```
Switch(config)# interface
Switch(config-if)# mvr type receiver
```

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

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

```
Switch(config)# interface
Switch(config-if)# mvr immediate
```

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

```
Switch(config)# interface
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

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

■ **mvr (interface configuration)**

Related Commands	Command	Description
	<b>mvr (global configuration)</b>	Enables and configures multicast VLAN registration on the switch.
	<b>show mvr</b>	Displays MVR global parameters or port parameters.
	<b>show mvr interface</b>	Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. Also displays all MVR groups of which the interface is a member.
	<b>show mvr members</b>	Displays all receiver ports that are members of an MVR multicast group.

# network-policy

Use the **network-policy** interface configuration command to apply a network-policy profile to an interface. Use the **no** form of this command to remove the policy.

**network-policy** *profile number*

**no network-policy**

<b>Syntax Description</b>	<i>profile number</i>	Specify the network-policy profile number.
<b>Defaults</b>	No network-policy profiles are applied.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.
<b>Usage Guidelines</b>	<p>Use the <b>network-policy</b> <i>profile number</i> interface configuration command to apply a profile to an interface.</p> <p>If you first configure a network-policy profile on an interface, you cannot apply the <b>switchport voice vlan</b> command on the interface. If <b>switchport voice vlan</b> <i>vlan-id</i> is already configured on an interface, you can apply a network-policy profile on the interface. The interface then has the voice or voice-signaling VLAN network-policy profile applied on the interface.</p>	
<b>Examples</b>	<p>This example shows how to apply network-policy profile 60 to an interface:</p> <pre>Switch(config)# interface_id Switch(config-if)# network-policy 60</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">network-policy profile (global configuration)</a>	Creates the network-policy profile.
	<a href="#">network-policy profile (network-policy configuration)</a>	Configures the attributes of network-policy profiles.
	<a href="#">show network-policy profile</a>	Displays the configured network-policy profiles.

---

**■ network-policy profile (global configuration)**

# network-policy profile (global configuration)

Use the **network-policy profile** global configuration command to create a network-policy profile and to enter network-policy configuration mode. Use the **no** form of this command to delete the policy and to return to global configuration mode.

**network-policy profile** *profile number*

**no network-policy profile** *profile number*

<b>Syntax Description</b>	<i>profile number</i>	Specify the network-policy profile number. The range is 1 to 4294967295.
---------------------------	-----------------------	--

<b>Defaults</b>	No network-policy profiles are defined.
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	<p>Use the <b>network-policy profile</b> global configuration command to create a profile and to enter network-policy profile configuration mode.</p> <p>To return to the privileged EXEC mode from the network-policy profile configuration mode, enter the <b>exit</b> command.</p> <p>When you are in network-policy profile configuration mode, you can create the profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.</p> <p>These profile attributes are then contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) <b>network-policy</b> time-length-value (TLV).</p>
-------------------------	--

<b>Examples</b>	This example shows how to create network-policy profile 60:
	<pre>Switch(config)# network-policy profile 60 Switch(config-network-policy)#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>network-policy</b>	Applies a network-policy to an interface.
	<b>network-policy profile (network-policy configuration)</b>	Configures the attributes of network-policy profiles.
	<b>show network-policy profile</b>	Displays the configured network-policy profiles.

# network-policy profile (network-policy configuration)

Use the **network-policy profile** configuration mode command to configure the network-policy profile created by using the **network-policy profile** global configuration command. Use the **no** form of this command without additional parameters to delete a profile. Use the **no** form with parameters to change its configured attributes.

```
network-policy profile profile number {voice | voice-signaling} vlan [vlan-id {cos cvalue | dscp dvalue}] | [[dot1p {cos cvalue | dscp dvalue}] | none | untagged]
```

```
no network-policy profile profile number {voice | voice-signaling} vlan [vlan-id | {cos cvalue} | {dscp dvalue}] | [[dot1p {cos cvalue} | {dscp dvalue}] | none | untagged]
```

## Syntax Description

<b>voice</b>	Specify the voice application type.
<b>voice-signaling</b>	Specify the voice-signaling application type.
<b>vlan</b>	Specify the native VLAN for voice traffic.
<i>vlan-id</i>	(Optional) Specify the VLAN for voice traffic. The range is 1 to 4094.
<b>cos</b> <i>cvalue</i>	(Optional) Specify the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
<b>dscp</b> <i>dvalue</i>	(Optional) Specify the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
<b>dot1p</b>	(Optional) Configure the telephone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
<b>none</b>	(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
<b>untagged</b>	(Optional) Configure the telephone to send untagged voice traffic. This is the default for the telephone.

## Defaults

No network policies are defined.

## Command Modes

Network-policy configuration

## Command History

<b>Release</b>	<b>Modification</b>
12.2(50)SE	This command was introduced.

---

**■ network-policy profile (network-policy configuration)**
**Usage Guidelines**

Use the **network-policy profile** command to configure the attributes of a network-policy profile.

The **voice** application type is for dedicated IP telephones and similar devices that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security through isolation from data applications.

The **voice-signaling** application type is for network topologies that require a different policy for voice signaling than for voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **voice policy** TLV.

This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
```

This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>network-policy</b></a>	Applies a network-policy to an interface.
<a href="#"><b>network-policy profile (global configuration)</b></a>	Creates the network-policy profile.
<a href="#"><b>show network-policy profile</b></a>	Displays the configured network-policy profiles.

## nmsp

Use the **nmsp** global configuration command to enable Network Mobility Services Protocol (NMSP) on the switch. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting.

**nmsp {enable | {notification interval {attachment | location} interval-seconds}}**

**no nmsp {enable | {notification interval {attachment | location} interval-seconds}}**

Syntax Description	<b>enable</b> Enable the NMSP features on the switch. <b>notification interval</b> Specify the NMSP notification interval. <b>attachment</b> Specify the attachment notification interval. <b>location</b> Specify the location notification interval. <i>interval-seconds</i> Duration in seconds before a switch sends the MSE the location or attachment updates. The range is 1 to 30; the default is 30.								
<b>Defaults</b>	NMSP is disabled.								
<b>Command Modes</b>	Global configuration								
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>12.2(50)SE</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	12.2(50)SE	This command was introduced.				
Release	Modification								
12.2(50)SE	This command was introduced.								
<b>Usage Guidelines</b>	Use the <b>nmsp</b> global configuration command to enable the switch to send NMSP location and attachment notifications to a Cisco Mobility Services Engine (MSE).								
<b>Examples</b>	<p>This example shows how to enable NMSP on a switch and set the location notification time to 10 seconds:</p> <pre>Switch(config)# vlan enable Switch(config)# vlan notification interval location 10</pre>								
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td><a href="#">clear nmsp statistics</a></td><td>Clears the NMSP statistic counters.</td></tr> <tr> <td><a href="#">nmsp attachment suppress</a></td><td>Suppresses reporting attachment information from a specified interface.</td></tr> <tr> <td><a href="#">show nmsp</a></td><td>Displays the NMSP information.</td></tr> </tbody> </table>	Command	Description	<a href="#">clear nmsp statistics</a>	Clears the NMSP statistic counters.	<a href="#">nmsp attachment suppress</a>	Suppresses reporting attachment information from a specified interface.	<a href="#">show nmsp</a>	Displays the NMSP information.
Command	Description								
<a href="#">clear nmsp statistics</a>	Clears the NMSP statistic counters.								
<a href="#">nmsp attachment suppress</a>	Suppresses reporting attachment information from a specified interface.								
<a href="#">show nmsp</a>	Displays the NMSP information.								

**nmsp attachment suppress**

# nmsp attachment suppress

Use the **nmsp attachment suppress** interface configuration mode command to suppress the reporting of attachment information from a specified interface. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to return to the default setting.

**nmsp attachment suppress**

**no nmsp attachment suppress**

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

**Defaults** This command has no default setting.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Use the **nmsp attachment suppress** interface configuration command to configure an interface to not send location and attachment notifications to a Cisco Mobility Services Engine (MSE).

**Examples** This example shows how to configure an interface to not send attachment information to the MSE:

```
Switch(config)# switch interface interface-id
Switch(config-if)# nmsp attachment suppress
```

Related Commands	Command	Description
	<b>nmsp</b>	Enables Network Mobility Services Protocol (NMSP) on the switch.
	<b>show nmsp</b>	Displays the NMSP information.

# no authentication logging verbose

Use the **no authentication logging verbose** global configuration command on the switch stack or on a standalone switch to filter detailed information from authentication system messages.

## **no authentication logging verbose**

**Defaults** All details are displayed in the system messages.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** This command filters details, such as anticipated success, from authentication system messages.

**Examples** To filter verbose authentication system messages:

```
Switch(config)# no authentication logging verbose
```

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

Related Commands	Command	Description
	<b>no authentication logging verbose</b>	Filters details from authentication system messages.
	<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
	<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

**no dot1x logging verbose**

# no dot1x logging verbose

Use the **no dot1x logging verbose** global configuration command on the switch stack or on a standalone switch to filter detailed information from 802.1x system messages.

## **no dot1x logging verbose**

---

**Defaults**

All details are displayed in the system messages.

---

**Syntax Description**

This command has no arguments or keywords.

---

**Command Modes**

Global configuration

---

**Command History**

Release	Modification
12.2(55)SE	This command was introduced.

---



---

**Usage Guidelines**

This command filters details, such as anticipated success, from 802.1x system messages.

---

**Examples**

To filter verbose 802.1x system messages:

```
Switch(config)# no dot1x logging verbose
```

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

---

**Related Commands**

Command	Description
<b>no authentication logging verbose</b>	Filters details from authentication system messages.
<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

---

# no mab logging verbose

Use the **no mab logging verbose** global configuration command on the switch stack or on a standalone switch to filter detailed information from MAC authentication bypass (MAB) system messages.

## **no mab logging verbose**

**Defaults** All details are displayed in the system messages.

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

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(55)SE	This command was introduced.

**Usage Guidelines** This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages.

**Examples** To filter verbose MAB system messages:

```
Switch(config)# no mab logging verbose
```

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

Related Commands	Command	Description
	<b>no authentication logging verbose</b>	Filters details from authentication system messages.
	<b>no dot1x logging verbose</b>	Filters details from 802.1x system messages.
	<b>no mab logging verbose</b>	Filters details from MAC authentication bypass (MAB) system messages.

**pagp learn-method**

# pagp learn-method

Use the **pagp learn-method** interface configuration command to learn the source address of incoming packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

**pagp learn-method {aggregation-port | physical-port}**

**no pagp learn-method**

<b>Syntax Description</b>	<b>aggregation-port</b> Specify address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives. <b>physical-port</b> Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.
---------------------------	---

**Defaults**      The default is aggregation-port (logical port channel).

**Command Modes**      Interface configuration

## Command History

**Usage Guidelines**      The learn method must be configured the same at both ends of the link.



**Note**      The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

## Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">pagp port-priority</a>	Selects a port over which all traffic through the EtherChannel is sent.
<a href="#">show pagp</a>	Displays PAgP channel-group information.
<a href="#">show running-config</a>	Displays the current operating configuration.

**pagg port-priority**

# pagg port-priority

Use the **pagg port-priority** interface configuration command to select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. Use the **no** form of this command to return to the default setting.

**pagg port-priority *priority***

**no pagg port-priority**

---

<b>Syntax Description</b>	<i>priority</i>	A priority number ranging from 0 to 255.
---------------------------	-----------------	--

---

<b>Defaults</b>	The default is 128.
-----------------	---------------------

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

---

## Command History

<b>Usage Guidelines</b>	The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.
-------------------------	--



The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagg learn-method** and the **pagg port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagg learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagg learn-method** interface configuration command only in this situation.

---

<b>Examples</b>	This example shows how to set the port priority to 200:
-----------------	---

```
Switch(config-if)# pagg port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagg channel-group-number internal** privileged EXEC command.

---

## Related Commands

Command	Description
<b>pagp learn-method</b>	Provides the ability to learn the source address of incoming packets.
<b>show pagp</b>	Displays PAgP channel-group information.
<b>show running-config</b>	Displays the current operating configuration.

---

 ■ permit (ARP access-list configuration)

## permit (ARP access-list configuration)

Use the **permit** Address Resolution Protocol (ARP) access-list configuration command to permit an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings. Use the **no** form of this command to remove the specified access control entry (ACE) from the access control list.

```
permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
no permit {[request] ip {any | host sender-ip | sender-ip sender-ip-mask} mac {any | host sender-mac | sender-mac sender-mac-mask} | response ip {any | host sender-ip | sender-ip sender-ip-mask} [{any | host target-ip | target-ip target-ip-mask}] mac {any | host sender-mac | sender-mac sender-mac-mask} [{any | host target-mac | target-mac target-mac-mask}]} [log]
```

Syntax Description	
<b>request</b>	(Optional) Requests a match for the ARP request. When <b>request</b> is not specified, matching is performed against all ARP packets.
<b>ip</b>	Specify the sender IP address.
<b>any</b>	Accept any IP or MAC address.
<b>host sender-ip</b>	Accept the specified sender IP address.
<b>sender-ip</b>	Accept the specified range of sender IP addresses.
<b>sender-ip-mask</b>	
<b>mac</b>	Specify the sender MAC address.
<b>host sender-mac</b>	Accept the specified sender MAC address.
<b>sender-mac</b>	Accept the specified range of sender MAC addresses.
<b>sender-mac-mask</b>	
<b>response ip</b>	Define the IP address values for the ARP responses.
<b>host target-ip</b>	(Optional) Accept the specified target IP address.
<b>target-ip target-ip-mask</b>	(Optional) Accept the specified range of target IP addresses.
<b>mac</b>	Specify the MAC address values for the ARP responses.
<b>host target-mac</b>	(Optional) Accept the specified target MAC address.
<b>target-mac</b>	(Optional) Accept the specified range of target MAC addresses.
<b>target-mac-mask</b>	
<b>log</b>	(Optional) Log a packet when it matches the ACE. Matches are logged if you also configure the <b>matchlog</b> keyword in the <a href="#">ip arp inspection vlan logging</a> global configuration command.

---

 ■ **Defaults** There are no default settings.

---

 ■ **Command Modes** ARP access-list configuration

Command History	Release	Modification
	12.2(20)SE	This command was introduced.

**Usage Guidelines** You can add permit clauses to forward ARP packets based on some matching criteria.

**Examples** This example shows how to define an ARP access list and to permit both ARP requests and ARP responses from a host with an IP address of 1.1.1.1 and a MAC address of 0000.0000.abcd:

```
Switch(config)# arp access-list static-hosts
Switch(config-arp-nacl)# permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch(config-arp-nacl)# end
```

You can verify your settings by entering the **show arp access-list** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">arp access-list</a>	Defines an ARP access control list (ACL).
	<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the DHCP bindings.
	<a href="#">ip arp inspection filter vlan</a>	Permits ARP requests and responses from a host configured with a static IP address.
	<a href="#">show arp access-list</a>	Displays detailed information about ARP access lists.

**■ permit (MAC access-list configuration)**

# permit (MAC access-list configuration)

Use the **permit** MAC access-list configuration command to allow non-IP traffic to be forwarded if the conditions are matched. Use the **no** form of this command to remove a permit condition from the extended MAC access list.

```
{permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]

no {permit | deny} {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} [type mask | cos cos | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp]
```



**Note** Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

**Syntax Description**

<b>any</b>	Keyword to specify to deny any source or destination MAC address.
<b>host src-MAC-addr   src-MAC-addr mask</b>	Define a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
<b>host dst-MAC-addr   dst-MAC-addr mask</b>	Define a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
<b>type mask</b>	(Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. <ul style="list-style-type: none"> <li>• <i>type</i> is 0 to 65535, specified in hexadecimal.</li> <li>• <i>mask</i> is a mask of <i>don't care</i> bits applied to the Ethertype before testing for a match.</li> </ul>
<b>aarp</b>	(Optional) Select EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
<b>amber</b>	(Optional) Select EtherType DEC-Amber.
<b>cos cos</b>	(Optional) Select an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the <b>cos</b> option is configured.
<b>dec-spanning</b>	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
<b>decnet-iv</b>	(Optional) Select EtherType DECnet Phase IV protocol.
<b>diagnostic</b>	(Optional) Select EtherType DEC-Diagnostic.
<b>dsm</b>	(Optional) Select EtherType DEC-DSM.
<b>etype-6000</b>	(Optional) Select EtherType 0x6000.
<b>etype-8042</b>	(Optional) Select EtherType 0x8042.
<b>lat</b>	(Optional) Select EtherType DEC-LAT.
<b>lavc-sca</b>	(Optional) Select EtherType DEC-LAVC-SCA.

<b>lsap lsap-number mask</b>	(Optional) Use the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.  The <i>mask</i> is a mask of <i>don't care</i> bits applied to the LSAP number before testing for a match.
<b>mop-console</b>	(Optional) Select EtherType DEC-MOP Remote Console.
<b>mop-dump</b>	(Optional) Select EtherType DEC-MOP Dump.
<b>msdos</b>	(Optional) Select EtherType DEC-MSDOS.
<b>mumps</b>	(Optional) Select EtherType DEC-MUMPS.
<b>netbios</b>	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
<b>vines-echo</b>	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
<b>vines-ip</b>	(Optional) Select EtherType VINES IP.
<b>xns-idp</b>	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite.

To filter IPX traffic, you use the *type mask* or **lsap lsap mask** keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in [Table 2-22](#).

**Table 1-22 IPX Filtering Criteria**

<b>IPX Encapsulation Type</b>		<b>Filter Criterion</b>
<b>Cisco IOS Name</b>	<b>Novell Name</b>	
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

#### Defaults

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

#### Command Modes

MAC access-list configuration

#### Command History

#### Usage Guidelines

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

**■ permit (MAC access-list configuration)**

For more information about MAC-named extended access lists, see the software configuration guide for this release.

**Examples**

This example shows how to define the MAC-named extended access list to allow NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>deny (MAC access-list configuration)</b></a>	Denies non-IP traffic to be forwarded if conditions are matched.
<a href="#"><b>mac access-list extended</b></a>	Creates an access list based on MAC addresses for non-IP traffic.
<a href="#"><b>show access-lists</b></a>	Displays access control lists configured on a switch.

# police

Use the **police** policy-map class configuration command to define a policer for classified traffic. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. Use the **no** form of this command to remove an existing policer.

**police *rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]***

**no police *rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]***

Syntax Description	
<i>rate-bps</i>	Specify the average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.
<i>burst-byte</i>	Specify the normal burst size in bytes. The range is 8000 to 1000000.
<b>exceed-action drop</b>	(Optional) When the specified rate is exceeded, specify that the switch drop the packet.
<b>exceed-action policed-dscp-transmit</b>	(Optional) When the specified rate is exceeded, specify that the switch changes the Differentiated Services Code Point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet.

## Defaults

No policers are defined.

## Command Modes

Policy-map class configuration

## Command History

### Usage Guidelines

When configuring hierarchical policy maps, you can only use the **police** policy-map command in a secondary interface-level policy map.

The port ASIC device, which controls more than one physical port, supports 256 policers (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of user-configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Policing uses a token-bucket algorithm. You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the *burst-byte* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. You configure how quickly (the average rate) the tokens are removed from the bucket by using the *rate-bps* option of the **police** policy-map class configuration command or the **mls qos aggregate-policer** global configuration command. For more information, see the software configuration guide for this release.

**police****Examples**

This example shows how to configure a policer that drops packets if traffic exceeds 1 Mb/s average rate with a burst size of 20 KB. The DSCPs of incoming packets are trusted, and there is no packet modification.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action drop
Switch(config-pmap-c)# exit
```

This example shows how to configure a policer, which marks down the DSCP values with the values defined in policed-DSCP map and sends the packet:

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>class</b></a>	Defines a traffic classification match criteria (through the <b>police</b> , <b>set</b> , and <b>trust</b> policy-map class configuration commands) for the specified class-map name.
<a href="#"><b>mls qos map policed-dscp</b></a>	Applies a policed-DSCP map to a DSCP-trusted port.
<a href="#"><b>policy-map</b></a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#"><b>set</b></a>	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
<a href="#"><b>show policy-map</b></a>	Displays quality of service (QoS) policy maps.
<a href="#"><b>trust</b></a>	Defines a trust state for traffic classified through the <b>class</b> policy-map configuration or the <b>class-map</b> global configuration command.

# police aggregate

Use the **police aggregate** policy-map class configuration command to apply an aggregate policer to multiple classes in the same policy map. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. Use the **no** form of this command to remove the specified policer.

**police aggregate *aggregate-policer-name***

**no police aggregate *aggregate-policer-name***

<b>Syntax Description</b>	<i>aggregate-policer-name</i>	Name of the aggregate policer.
<b>Defaults</b>	No aggregate policers are defined.	
<b>Command Modes</b>	Policy-map class configuration	
<b>Command History</b>		
<b>Usage Guidelines</b>	<p>The port ASIC device, which controls more than one physical port, supports 256 policers (255 user-configurable policers plus 1 policer reserved for internal use). The maximum number of user-configurable policers supported per port is 63. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port. There is no guarantee that a port will be assigned to any policer.</p> <p>You set aggregate policer parameters by using the <b>mls qos aggregate-policer</b> global configuration command. You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps.</p> <p>To return to policy-map configuration mode, use the <b>exit</b> command. To return to privileged EXEC mode, use the <b>end</b> command.</p> <p>You cannot configure aggregate policers in hierarchical policy maps.</p>	

**police aggregate****Examples**

This example shows how to define the aggregate policer parameters and to apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate agg_policer2
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show mls qos aggregate-policer** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>mls qos aggregate-policer</b></a>	Defines policer parameters, which can be shared by multiple classes within a policy map.
<a href="#"><b>show mls qos aggregate-policer</b></a>	Displays the quality of service (QoS) aggregate policer configuration.

# policy-map

Use the **policy-map** global configuration command to create or modify a policy map that can be attached to multiple physical ports and to enter policy-map configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

<b>Syntax Description</b>	<i>policy-map-name</i> Name of the policy map.
<b>Defaults</b>	No policy maps are defined. The default behavior is to set the Differentiated Services Code Point (DSCP) to 0 if the packet is an IP packet and to set the class of service (CoS) to 0 if the packet is tagged. No policing is performed.
<b>Command Modes</b>	Global configuration
<b>Command History</b>	
<b>Usage Guidelines</b>	<p>After entering the <b>policy-map</b> command, you enter policy-map configuration mode, and these configuration commands are available:</p> <ul style="list-style-type: none"> <li>• <b>class</b>: defines the classification match criteria for the specified class map. For more information, see the “<a href="#">class</a>” section on page <a href="#">2-86</a>.</li> <li>• <b>description</b>: describes the policy map (up to 200 characters).</li> <li>• <b>exit</b>: exits policy-map configuration mode and returns you to global configuration mode.</li> <li>• <b>no</b>: removes a previously defined policy map.</li> <li>• <b>rename</b>: renames the current policy map.</li> </ul> <p>To return to global configuration mode, use the <b>exit</b> command. To return to privileged EXEC mode, use the <b>end</b> command.</p> <p>Before configuring policies for classes whose match criteria are defined in a class map, use the <b>policy-map</b> command to specify the name of the policy map to be created, added to, or modified. Entering the <b>policy-map</b> command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.</p> <p>You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the <b>class-map</b> global configuration and <b>match</b> class-map configuration commands. You define packet classification on a physical-port basis.</p> <p>Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.</p>

**■ policy-map****Examples**

This example shows how to create a policy map called *policy1*. When attached to the ingress port, it matches all the incoming traffic defined in *class1*, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

This example shows how to configure multiple classes in a policy map called *policymap2*:

```
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 100000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 100000 20000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp 0 (no policer)
Switch(config-pmap-c)# exit
```

This example shows how to delete *policymap2*:

```
Switch(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">class</a>	Defines a traffic classification match criteria (through the <b>police</b> , <b>set</b> , and <b>trust</b> policy-map class configuration command) for the specified class-map name.
<a href="#">class-map</a>	Creates a class map to be used for matching packets to the class whose name you specify.
<a href="#">service-policy</a>	Applies a policy map to a port.
<a href="#">show policy-map</a>	Displays QoS policy maps.

# port-channel load-balance

Use the **port-channel load-balance** global configuration command to set the load-distribution method among the ports in the EtherChannel. Use the **no** form of this command to return to the default setting.

**port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}**

**no port-channel load-balance**

Syntax Description	<b>dst-ip</b> Load distribution is based on the destination host IP address. <b>dst-mac</b> Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel. <b>src-dst-ip</b> Load distribution is based on the source and destination host IP address. <b>src-dst-mac</b> Load distribution is based on the source and destination host MAC address. <b>src-ip</b> Load distribution is based on the source host IP address. <b>src-mac</b> Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
--------------------	---

**Defaults** The default is **src-mac**.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** For information about when to use these forwarding methods, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

**Examples** This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Related Commands	Command	Description
	<b>interface port-channel</b>	Accesses or creates the port channel.
	<b>show etherchannel</b>	Displays EtherChannel information for a channel.
	<b>show running-config</b>	Displays the current operating configuration.

**power inline**

# power inline

Use the **power inline** interface configuration command to configure the power management mode on the Power over Ethernet (PoE) ports. Use the **no** form of this command to return to the default settings.

```
power inline { auto [max max-wattage] | never | police [action {errdisable | log}] | static [max max-wattage]}
```

```
no power inline {auto | never | police | static}
```

Syntax Description	
<b>auto</b>	Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection.
<b>max max-wattage</b>	(Optional) Limit the power allowed on the port. The range is 4000 to 15400 milliwatts. If no value is specified, the maximum is allowed.
<b>never</b>	Disable device detection, and disable power to the port.
<b>static</b>	Enable powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device.

## Defaults

The default is **auto** (enabled).

The maximum wattage is 15400 milliwatts.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, this error message appears:

```
Switch(config)# interface
Switch(config-if)# power inline auto
^
% Invalid input detected at '^' marker.
```

All PoE-capable switch ports are IEEE 802.3 af-compliant.

Use the **max max-wattage** option to disallow higher-power powered devices. With this configuration, when the powered device sends Cisco Discovery Protocol (CDP) messages requesting more power than the maximum wattage, the switch removes power from the port. If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.



**Note** The switch never powers any Class 0 or Class 3 device if the **power inline max max-wattage** command is configured for less than 15.4 W.

If the switch denies power to a powered device (the powered device requests more power through CDP messages or if the IEEE class maximum is greater than the maximum wattage), the PoE port is in a power-deny state. The switch generates a system message, and the Oper column in the **show power inline** user EXEC command output shows *power-deny*.

Use the **power inline static max max-wattage** command to give a port high priority. The switch allocates PoE to a port configured in static mode before allocating power to a port configured in auto mode. The switch reserves power for the static port when it is configured rather than upon device discovery. The switch reserves the power on a static port even when there is no connected device and whether or not the port is in a shutdown or in a no shutdown state. The switch allocates the configured maximum wattage to the port, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed power when it is connected to a static port. However, if the powered device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shut down.

If the switch cannot pre-allocate power when a port is in static mode (for example, because the entire power budget is already allocated to other auto or static ports), this message appears: Command rejected: power inline static: pwr not available. The port configuration remains unchanged.

When you configure a port by using the **power inline auto** or the **power inline static** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.

When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

If a port has a Cisco powered device connected to it, you should not use the **power inline never** command to configure the port. A false link-up can occur on the port, placing it into an error-disabled state.

## Examples

This example shows how to enable detection of a powered device and to automatically power a PoE port:

```
Switch(config)# interface
Switch(config-if)# power inline auto
```

This example shows how to configure a PoE port to allow a Class 1 or a Class 2 powered device:

```
Switch(config)# interface
Switch(config-if)# power inline auto max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port:

```
Switch(config)# interface
Switch(config-if)# power inline never
```

You can verify your settings by entering the **show power inline** user EXEC command.

## Related Commands

**power inline**

Command	Description
<b>logging event</b>	Enables the logging of PoE events.
<b>power-inline-status</b>	
<b>show controllers</b>	Displays the values in the registers of the specified PoE controller.
<b>power inline</b>	
<b>show power inline</b>	Displays the PoE status for the specified PoE port or for all PoE ports.

# power inline consumption

Use the **power inline consumption** global or interface configuration command to override the amount of power specified by the IEEE classification for the device by specifying the wattage used by each powered device. Use the **no** form of this command to return to the default power setting.

**power inline consumption default *wattage***

**no power inline consumption default**



**Note**

---

The **default** keyword appears only in the global configuration command.

---

**Syntax Description**

<i>wattage</i>	Specify the power that the switch budgets for the port. The range is 4000 to 15400 milliwatts.
----------------	--

---

**Defaults**

The default power is 15400 milliwatts on each Power over Ethernet (PoE) port.

**Command Modes**

Global configuration

Interface configuration

**Command History**

**Usage Guidelines**

When Cisco powered devices are connected to PoE ports, the switch uses Cisco Discovery Protocol (CDP) to determine the *actual* power consumption of the devices, and the switch adjusts the power budget accordingly. This does not apply to IEEE third-party powered devices. For these devices, when the switch grants a power request, the switch adjusts the power budget according to the powered-device IEEE classification. If the powered device is a Class 0 (class status unknown) or a Class 3, the switch budgets 15400 milliwatts for the device, regardless of the actual amount of power needed. If the powered device reports a higher class than its actual consumption or does not support power classification (defaults to Class 0), the switch can power fewer devices because it uses the IEEE class information to track the global power budget.

By using the **power inline consumption *wattage*** configuration command, you can override the default power requirement specified by the IEEE classification. The difference between what is mandated by the IEEE classification and what is actually needed by the device is reclaimed into the global power budget for use by additional devices. You can then extend the switch power budget and use it more effectively.

For example, if the switch budgets 15400 milliwatts on each PoE port, you can connect only 24 Class 0 powered devices. If your Class 0 device power requirement is actually 5000 milliwatts, you can set the consumption wattage to 5000 milliwatts and connect up to 48 devices. The total PoE output power available on a 24-port or 48-port switch is 370,000 milliwatts.



**Caution**

---

You should carefully plan your switch power budget and make certain not to oversubscribe the power supply.

---

**power inline consumption**

When you enter the **power inline consumption default** *wattage* or the **no power inline consumption default** global configuration command, or the **power inline consumption** *wattage* or the **no power inline consumption** interface configuration command, this caution message appears.

%CAUTION: Interface *interface-id*: Misconfiguring the 'power inline consumption/allocation' command may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply. Refer to documentation.

**Note**

When you manually configure the power budget, you must also consider the power loss over the cable between the switch and the powered device.

For more information about the IEEE power classifications, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

This command is supported only on PoE-capable ports. If you enter this command on a switch or port that does not support PoE, an error message appears.

**Examples**

By using the global configuration command, this example shows how to configure the switch to budget 5000 milliwatts to each PoE port:

```
Switch(config)# power inline consumption default 5000
```

%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation' command may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply. Refer to documentation.

By using the interface configuration command, this example shows how to configure the switch to budget 12000 milliwatts to the powered device connected to a specific PoE port:

```
Switch(config)# interface
```

```
Switch(config-if)# power inline consumption 12000
```

%CAUTION: Interface Gi1/0/2: Misconfiguring the 'power inline consumption/allocation' command may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply. Refer to documentation.

You can verify your settings by entering the **show power inline consumption** privileged EXEC command.

**Related Commands**

Command	Description
<b>power inline</b>	Configures the power management mode on PoE ports.
<b>show power inline</b>	Displays the PoE status for the specified PoE port or for all PoE ports.

# priority-queue

Use the **priority-queue** interface configuration command to enable the egress expedite queue on a port. Use the **no** form of this command to return to the default setting.

**priority-queue out**

**no priority-queue out**

<b>Syntax Description</b>	<b>out</b> Enable the egress expedite queue.
<b>Defaults</b>	The egress expedite queue is disabled.
<b>Command Modes</b>	Interface configuration
<b>Command History</b>	
<b>Usage Guidelines</b>	<p>When you configure the <b>priority-queue out</b> command, the shaped round robin (SRR) weight ratios are affected because there is one fewer queue participating in SRR. This means that <i>weight1</i> in the <b>srr-queue bandwidth shape</b> or the <b>srr-queue bandwidth shape</b> interface configuration command is ignored (not used in the ratio calculation). The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced.</p> <p>Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:</p> <ul style="list-style-type: none"> <li>• If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.</li> <li>• If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.</li> <li>• If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services the queue in shared mode.</li> </ul>
<b>Examples</b>	<p>This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.</p> <pre>Switch(config)# interface Switch(config-if)# srr-queue bandwidth shape 25 0 0 0 Switch(config-if)# srr-queue bandwidth share 30 20 25 25 Switch(config-if)# priority-queue out</pre>

**■ priority-queue**

This example shows how to disable the egress expedite queue after the SRR shaped and shared weights are configured. The shaped mode overrides the shared mode.

```
Switch(config)# interface
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# no priority-queue out
```

You can verify your settings by entering the **show mls qos interface *interface-id* queueing** or the **show running-config** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show mls qos interface <i>interface-id</i> queueing</b></a>	Displays the queueing strategy (SRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.
<a href="#"><b>srr-queue bandwidth shape</b></a>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
<a href="#"><b>srr-queue bandwidth share</b></a>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

## psp

To control the rate at which protocol packets are sent to the switch, use the **psp** global configuration command to specify the upper threshold for the packet flow rate. The supported protocols are Address Resolution Protocol (ARP), ARP snooping, Dynamic Host Configuration Protocol (DHCP) v4, DHCP snooping, Internet Group Management Protocol (IGMP), and IGMP snooping. To disable protocol storm protection, use the **no** version of the command.

```
psp {arp | dhcp | igmp} pps value
```

```
no psp {arp | dhcp | igmp}
```

### Syntax Description

<b>arp</b>	Set protocol packet flow rate for ARP and ARP snooping.
<b>dhcp</b>	Set protocol packet flow rate for DHCP and DHCP snooping.
<b>igmp</b>	Set protocol packet flow rate for IGMP and IGMP snooping.
<b>pps value</b>	Specify the threshold value for the number of packets per second. If the traffic exceeds this value, protocol storm protection is enforced. The range is from 5 to 50 packets per second.

### Defaults

Protocol storm protection is disabled by default.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(58)SE	This command was introduced.

### Usage Guidelines

To set error-disable detection protocol storm protection, use the **errdisable detect cause psp** global configuration command.

When protocol storm protection is configured, a counter records the number of dropped packets. To see the number of dropped packets for a specific protocol, use the **show psp statistics {arp | dhcp | igmp}** privileged EXEC command. To see the number of dropped packets for all protocols, use the **show psp statistics all** command. To clear the counter for a protocol, use the **clear psp counter [arp | dhcp | igmp]** command.

### Related Commands

Command	Description
<b>show psp config</b>	Displays the protocol storm protection configuration.
<b>show psp statistics</b>	Displays the number of dropped packets.
<b>clear psp counter</b>	Clears the counter of dropped packets.
<b>errdisable detect cause psp</b>	Enables error-disable detection for protocol storm protection.

**queue-set**

# queue-set

Use the **queue-set** interface configuration command to map a port to a queue-set. Use the **no** form of this command to return to the default setting.

**queue-set** *qset-id*

**no queue-set** *qset-id*

---

<b>Syntax Description</b>	<i>qset-id</i> ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
---------------------------	--

---

<b>Defaults</b>	The queue-set ID is 1.
-----------------	------------------------

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

## Command History

For information about automatic generation of the queue-set ID with the **auto qos voip** command, see the “Usage Guidelines” section for the **auto qos voip** command.

<b>Examples</b>	This example shows how to map a port to queue-set 2:
-----------------	--

```
Switch(config)# interface
Switch(config-if)# queue-set 2
```

You can verify your settings by entering the **show mls qos interface [interface-id] buffers** privileged EXEC command.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>mls qos queue-set output buffers</b>	Allocates buffers to a queue-set.
	<b>mls qos queue-set output threshold</b>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	<b>show mls qos interface buffers</b>	Displays quality of service (QoS) information.

---

# radius-server dead-criteria

Use the **radius-server dead-criteria** global configuration command to configure the conditions that determine when a RADIUS server is considered unavailable or *dead*. Use the **no** form of this command to return to the default settings.

**radius-server dead-criteria [time seconds [tries number] | tries number]**

**no radius-server dead-criteria [time seconds [tries number] | tries number]**

<b>Syntax Description</b>	<b>time seconds</b> (Optional) Set the time in seconds during which the switch does not need to get a valid response from the RADIUS server. The range is from 1 to 120 seconds. <b>tries number</b> (Optional) Set the number of times that the switch does not get a valid response from the RADIUS server before the server is considered unavailable. The range is from 1 to 100.
---------------------------	--

## Defaults

The switch dynamically determines the *seconds* value that is from 10 to 60 seconds.

The switch dynamically determines the *tries* value that is from 10 to 100.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(25)SEE	This command was introduced.

## Usage Guidelines

We recommend that you configure the *seconds* and *number* parameters as follows:

- Use the **radius-server timeout** *seconds* global configuration command to specify the time in seconds during which the switch waits for a RADIUS server to respond before the IEEE 802.1x authentication times out. The switch dynamically determines the default *seconds* value that is from 10 to 60 seconds.
- Use the **radius-server retransmit** *retries* global configuration command to specify the number of times the switch tries to reach the radius servers before considering the servers to be unavailable. The switch dynamically determines the default *tries* value that is from 10 to 100.
- The *seconds* parameter is less than or equal to the number of retransmission attempts times the time in seconds before the IEEE 802.1x authentication times out.
- The *tries* parameter should be the same as the number of retransmission attempts.

## Examples

This example shows how to configure 60 as the **time** and 10 as the number of **tries**, the conditions that determine when a RADIUS server is considered unavailable

```
Switch(config)# radius-server dead-criteria time 60 tries 10
```

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

■ **radius-server dead-criteria**

Related Commands	Command	Description
	<b>dot1x critical (global configuration)</b>	Configures the parameters for the inaccessible authentication bypass feature.
	<b>dot1x critical (interface configuration)</b>	Enables the inaccessible authentication bypass feature on an interface and configures the access VLAN to which the switch assigns the critical port when the port is in the critical-authentication state.
	<b>radius-server retransmit <i>retries</i></b>	Specifies the number of times that the switch tries to reach the RADIUS servers before considering the servers to be unavailable.
	<b>radius-server timeout <i>seconds</i></b>	Specifies the time in seconds during which the switch waits for a RADIUS server to respond before the IEEE 802.1x authentication times out.
	<b>show running-config</b>	Displays the running configuration on the switch.

# radius-server host

Use the **radius-server host** global configuration command to configure the RADIUS server parameters, including the RADIUS accounting and authentication. Use the **no** form of this command to return to the default settings.

```
radius-server host ip-address [acct-port udp-port] [auth-port udp-port] [test username name]
[idle-time time] [ignore-acct-port] [ignore-auth-port]] [key string]
```

**no radius-server host ip-address**

## Syntax Description

<b>ip-address</b>	Specify the IP address of the RADIUS server.
<b>acct-port udp-port</b>	(Optional) Specify the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
<b>auth-port udp-port</b>	(Optional) Specify the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
<b>test username name</b>	(Optional) Enable automatic server testing of the RADIUS server status, and specify the username to be used.
<b>idle-time time</b>	(Optional) Set the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes.
<b>ignore-acct-port</b>	(Optional) Disables testing on the RADIUS-server accounting port.
<b>ignore-auth-port</b>	(Optional) Disables testing on the RADIUS-server authentication port.

The key is used to encrypt and decrypt RADIUS communication between the switch and the RADIUS daemon. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in this command. Leading spaces are ignored, but spaces within and at the end of the key are used. If there are spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.

## Defaults

The UDP port for the RADIUS accounting server is 1646.

The UDP port for the RADIUS authentication server is 1645.

Automatic server testing is disabled.

The idle time is 60 minutes (1 hour).

When the automatic testing is enabled, testing occurs on the accounting and authentication UDP ports.

The authentication and encryption key (*string*) is not configured.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(25)SEE	This command was introduced.

**radius-server host****Usage Guidelines**

We recommend that you configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values.

Use the **test username name** keywords to enable automatic server testing of the RADIUS server status and to specify the username to be used.

You can configure the authentication and encryption key by using the **radius-server host ip-address key string** or the **radius-server key {0 string | 7 string | string}** global configuration command. Always configure the key as the last item in this command.

**Examples**

This example shows how to configure 1500 as the UDP port for the accounting server and 1510 as the UDP port for the authentication server:

```
Switch(config)# radius-server host 1.1.1.1 acct-port 1500 auth-port 1510
```

This example shows how to configure the UDP port for the accounting server and the authentication server, enable automated testing of the RADIUS server status, specify the username to be used, and configure a key string:

```
Switch(config)# radius-server host 1.1.1.2 acct-port 800 auth-port 900 test username
aaafail idle-time 75 key abc123
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>dot1x critical (global configuration)</b></a>	Configures the parameters for the inaccessible authentication bypass feature.
<a href="#"><b>dot1x critical (interface configuration)</b></a>	Enables the inaccessible authentication bypass feature on an interface and configures the access VLAN to which the switch assigns the critical port when the port is in the critical-authentication state.
<a href="#"><b>radius-server key {0 string   7 string   string}</b></a>	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
<a href="#"><b>show running-config</b></a>	Displays the running configuration on the switch.

# rcommand

Use the **rcommand** user EXEC command on the cluster command switch to start a Telnet session and to execute commands on a cluster member switch from the cluster command switch. To end the session, enter the **exit** command.

```
rcommand {n | commander | mac-address hw-addr}
```

Syntax Description	
<b>n</b>	Provide the number that identifies a cluster member. The range is 0 to 15.
<b>commander</b>	Provide access to the cluster command switch from a cluster member switch.
<b>mac-address hw-addr</b>	MAC address of the cluster member switch.

**Command Modes** User EXEC

## Command History

### Usage Guidelines

This command is available only on the cluster command switch.

If the switch is the cluster command switch but the cluster member switch *n* does not exist, an error message appears. To get the switch number, enter the **show cluster members** privileged EXEC command on the cluster command switch.

You can use this command to access a cluster member switch from the cluster command-switch prompt or to access a cluster command switch from the member-switch prompt.

For Catalyst 2900 XL, 3500 XL, 2950, 2960, 2970, 3550, 3560, and 3750 switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the cluster command switch. For example, if you execute this command at user level on the cluster command switch, the cluster member switch is accessed at user level. If you use this command on the cluster command switch at privileged level, the command accesses the remote device at privileged level. If you use an intermediate enable-level lower than *privileged*, access to the cluster member switch is at user level.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the cluster command switch is at privilege level 15. If the cluster command switch is at privilege level 1, you are prompted for the password before being able to access the menu console. Cluster command switch privilege levels map to the cluster member switches running standard edition software as follows:

- If the cluster command switch privilege level is from 1 to 14, the cluster member switch is accessed at privilege level 1.
- If the cluster command switch privilege level is 15, the cluster member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

This command will not work if the vty lines of the cluster command switch have access-class configurations.

You are not prompted for a password because the cluster member switches inherited the password of the cluster command switch when they joined the cluster.

**Examples**

This example shows how to start a session with member 3. All subsequent commands are directed to member 3 until you enter the **exit** command or close the session.

```
Switch# rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch#
```

**Related Commands**

Command	Description
<a href="#">show cluster members</a>	Displays information about the cluster members.

# remote-span

Use the **remote-span** VLAN configuration command to configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN. Use the **no** form of this command to remove the RSPAN designation from the VLAN.

**remote-span**

**no remote-span**

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

**Defaults** No RSPAN VLANs are defined.

**Command Modes** VLAN configuration (config-VLAN)

## Command History

### Usage Guidelines

You can configure RSPAN VLANs only in config-VLAN mode (entered by using the **vlan** global configuration command), not the VLAN configuration mode entered by using the **vlan database** privileged EXEC command.

If VLAN Trunking Protocol (VTP) is enabled, the RSPAN feature is propagated by VTP for VLAN-IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

Before you configure the RSPAN **remote-span** command, use the **vlan** (global configuration) command to create the VLAN.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports are made inactive until the RSPAN feature is disabled.

**remote-span****Examples**

This example shows how to configure a VLAN as an RSPAN VLAN.

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN.

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan remote-span** user EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>monitor session</b>	Enables Switched Port Analyzer (SPAN) and RSPAN monitoring on a port and configures a port as a source or destination port.
<b>usb-inactivity-timeout</b>	Changes to config-vlan mode where you can configure VLANs 1 to 4094.

# renew ip dhcp snooping database

Use the **renew ip dhcp snooping database** privileged EXEC command to renew the DHCP snooping binding database.

```
renew ip dhcp snooping database [{flash:/filename | ftp://user:password@host/filename |
                                nvram:/filename | rcp://user@host/filename | tftp://host/filename}] [validation none]
```

<b>Syntax Description</b>	<b>flash:/filename</b> <b>Note</b> (Optional) Specify that the database agent or the binding file is in the flash memory.
	<b>ftp://user:password @host/filename</b> (Optional) Specify that the database agent or the binding file is on an FTP server.
	<b>nvram:/filename</b> (Optional) Specify that the database agent or the binding file is in the NVRAM.
	<b>rcp://user@host/filename</b> (Optional) Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.
	<b>tftp://host/filename</b> (Optional) Specify that the database agent or the binding file is on a TFTP server.
	<b>validation none</b> (Optional) Specify that the switch does not verify the cyclic redundancy check (CRC) for the entries in the binding file specified by the URL.

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** If you do not specify a URL, the switch tries to read the file from the configured URL.

**Examples** This example shows how to renew the DHCP snooping binding database without checking CRC values in the file:

```
Switch# renew ip dhcp snooping database validation none
```

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

Related Commands	Command	Description
	<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
	<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database.
	<a href="#">show ip dhcp snooping database</a>	Displays the status of the DHCP snooping database agent.

**■ reserved-only**

## reserved-only

Use the **reserved-only** DHCP pool configuration mode command to allocate only reserved addresses in the Dynamic Host Configuration Protocol (DHCP) address pool. Use the **no** form of the command to return to the default.

**reserved-only**

**no reserved-only**

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

**Defaults** The default is to not restrict pool addresses

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Entering the **reserved-only** command restricts assignments from the DHCP pool to preconfigured reservations. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool.

By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.

To access DHCP pool configuration mode, enter the **ip dhcp pool *name*** global configuration command.

**Examples** This example shows how to configure the DHCP pool to allocate only reserved addresses:

```
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

You can verify your settings by entering the **show ip dhcp pool** privileged EXEC command.

Related Commands	Command	Description
	<b>show ip dhcp pool</b>	Displays the DHCP address pools.

# rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include usage statistics about broadcast and multicast packets, and error statistics about cyclic redundancy check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

**rmon collection stats index [owner name]**

**no rmon collection stats index [owner name]**

<b>Syntax Description</b>	<i>index</i> Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535. <i>owner name</i> (Optional) Owner of the RMON collection.
---------------------------	--

**Defaults**      The RMON statistics collection is disabled.

**Command Modes**      Interface configuration

## Command History

**Usage Guidelines**      The RMON statistics collection command is based on hardware counters.

**Examples**      This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config-if)# rmon collection stats 2 owner root
```

You can verify your setting by entering the **show rmon statistics** privileged EXEC command.

Related Commands	Command	Description
	<b>show rmon statistics</b>	Displays RMON statistics.

---

 service password-recovery

# service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to hold down the **Mode** button and interrupt the bootup process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the bootup process is allowed only if the user agrees to set the system back to the default configuration.

**service password-recovery**

**no service password-recovery**

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

**Defaults** The password-recovery mechanism is enabled.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** As a system administrator, you can use the **no service password-recovery** command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration.

To use the password-recovery procedure, a user with physical access to the switch holds down the **Mode** button while the unit powers up and for a second or two after the LED above port 1X turns off. When the button is released, the system continues with initialization.

If the password-recovery mechanism is disabled, this message appears:

The password-recovery mechanism has been triggered, but is currently disabled. Access to the boot loader prompt through the password-recovery mechanism is disallowed at this point. However, if you agree to let the system be reset back to the default system configuration, access to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?

**Note**

If the user chooses not to reset the system to the default configuration, the normal bootup process continues, as if the **Mode button** had not been pressed. If you choose to reset the system to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted. If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the config file in a location away from the switch in case the end user uses the password recovery procedure and sets the system back to default values. Do not keep a backup copy of the config file on the switch.

If the switch is operating in VTP transparent mode, we recommend that you also save a copy of the *vlan.dat* file in a location away from the switch.

You can verify if password recovery is enabled or disabled by entering the **show version** privileged EXEC command.

**Examples**

This example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration.

```
Switch(config)# no service-password recovery  
Switch(config)# exit
```

**Related Commands**

Command	Description
<a href="#">show version</a>	Displays version information for the hardware and firmware.

**service-policy**

# service-policy

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the input of a physical port. Use the **no** form of this command to remove the policy map and port association.

**service-policy input policy-map-name**

**no service-policy input policy-map-name**

<b>Syntax Description</b>	<b>input policy-map-name</b> Apply the specified policy map to the input of a physical port.
---------------------------	--



**Note** Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers. The **output** keyword is also not supported.

<b>Defaults</b>	No policy maps are attached to the port.
-----------------	--

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

## Command History

Policy maps can be configured on physical ports.

You can apply a policy map to incoming traffic on a physical port.

Classification using a port trust state (for example, **mls qos trust [cos | dscp | ip-precedence]**) and a policy map (for example, **service-policy input policy-map-name**) are mutually exclusive. The last one configured overwrites the previous configuration.

<b>Examples</b>	This example shows how to apply <i>plcmap1</i> to an physical ingress port:
-----------------	---

```
Switch(config-if)# service-policy input plcmap1
```

This example shows how to remove *plcmap2* from a physical port:

```
Switch(config-if)# no service-policy input plcmap2
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>policy-map</b>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
	<b>show policy-map</b>	Displays QoS policy maps.
	<b>show running-config</b>	Displays the running configuration on the switch.

## set

Use the **set** policy-map class configuration command to classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet. Use the **no** form of this command to remove traffic classification.

```
set {dscp new-dscp | [ip] precedence new-precedence}
no set {dscp new-dscp | [ip] precedence new-precedence}
```

Syntax Description	<b>dscp new-dscp</b>	New DSCP value assigned to the classified traffic. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
	<b>[ip] precedence new-precedence</b>	New IP-precedence value assigned to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.

**Defaults** No traffic classification is defined.

**Command Modes** Policy-map class configuration

### Command History

**Usage Guidelines** If you have used the **set ip dscp** policy-map class configuration command, the switch changes this command to **set dscp** in the switch configuration. If you enter the **set ip dscp** policy-map class configuration command, this setting appears as **set dscp** in the switch configuration.

You can use the **set ip precedence** policy-map class configuration command or the **set precedence** policy-map class configuration command. This setting appears as **set ip precedence** in the switch configuration.

The **set** command is mutually exclusive with the **trust** policy-map class configuration command within the same policy map.

For the **set dscp new-dscp** or the **set ip precedence new-precedence** command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

### Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
```

```
Switch(config-pmap) # exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

#### Related Commands

Command	Description
<a href="#"><b>class</b></a>	Defines a traffic classification match criteria (through the <b>police</b> , <b>set</b> , and <b>trust</b> policy-map class configuration commands) for the specified class-map name.
<a href="#"><b>police</b></a>	Defines a policer for classified traffic.
<a href="#"><b>policy-map</b></a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#"><b>show policy-map</b></a>	Displays QoS policy maps.
<a href="#"><b>trust</b></a>	Defines a trust state for traffic classified through the <b>class</b> policy-map configuration command or the <b>class-map</b> global configuration command.

# setup

Use the **setup** privileged EXEC command to configure the switch with its initial configuration.

**setup**

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

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment
- Whether the switch will be used as the cluster command switch and the cluster name

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (?) key at a prompt.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in NVRAM or return to the setup program or the command-line prompt without saving it.

## Examples

This is an example of output from the **setup** command:

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
Enter host name [Switch]:host-name

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
```

entered, becomes encrypted in the configuration.  
Enter enable secret: *enable-secret-password*

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: *enable-password*

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: *terminal-password*

Configure SNMP Network Management? [no]: **yes**  
Community string [public]:

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	172.20.135.202	YES	NVRAM	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	up	down
<output truncated>					
Port-channel1	unassigned	YES	unset	up	down

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface **vlan1**:  
Configure IP on this interface? [yes]: **yes**  
IP address for this interface: *ip\_address*  
Subnet mask for this interface [255.0.0.0]: *subnet\_mask*

Would you like to enable as a cluster command switch? [yes/no]: **yes**

Enter cluster name: *cluster-name*

The following configuration command script was created:

```
hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!

cluster enable cluster-name
!
end
```

```
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

Related Commands	Command	Description
	<a href="#">show running-config</a>	Displays the running configuration on the switch.
	<a href="#">show version</a>	Displays version information for the hardware and firmware.

**setup express**

# setup express

Use the **setup express** global configuration command to enable Express Setup mode. Use the **no** form of this command to disable Express Setup mode.

**setup express**

**no setup express**

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

**Defaults** Express Setup is enabled.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

When Express Setup is enabled on a new (unconfigured) switch, pressing the Mode button for 2 seconds activates Express Setup. You can access the switch through an Ethernet port by using the IP address 10.0.0.1 and then can configure the switch with the web-based Express Setup program or the command-line interface (CLI)-based setup program.

When you press the Mode button for 2 seconds on a configured switch, the LEDs above the Mode button start blinking. If you press the Mode button for a total of 10 seconds, the switch configuration is deleted, and the switch reboots. The switch can then be configured like a new switch, either through the web-based Express Setup program or the CLI-based setup program.



### Note

As soon as you make any change to the switch configuration (including entering *no* at the beginning of the CLI-based setup program), configuration by Express Setup is no longer available. You can only run Express Setup again by pressing the Mode button for 10 seconds. This deletes the switch configuration and reboots the switch.

If Express Setup is active on the switch, entering the **write memory** or **copy running-configuration startup-configuration** privileged EXEC commands deactivates Express Setup. The IP address 10.0.0.1 is no longer valid on the switch, and your connection using this IP address ends.

The primary purpose of the **no setup express** command is to prevent someone from deleting the switch configuration by pressing the Mode button for 10 seconds.

---

**Examples**

This example shows how to enable Express Setup mode:

```
Switch(config)# setup express
```

You can verify that Express Setup mode is enabled by pressing the Mode button:

- On an unconfigured switch, the LEDs above the Mode button turn solid green after 3 seconds.
- On a configured switch, the mode LEDs begin blinking after 2 seconds and turn solid green after 10 seconds.

**Caution**

If you *hold* the Mode button down for a total of 10 seconds, the configuration is deleted, and the switch reboots.

---

This example shows how to disable Express Setup mode:

```
Switch(config)# no setup express
```

You can verify that Express Setup mode is disabled by pressing the Mode button. The mode LEDs do not turn solid green *or* begin blinking green if Express Setup mode is not enabled on the switch.

---

**Related Commands**

Command	Description
<a href="#"><b>show setup express</b></a>	Displays if Express Setup mode is active.

---

**show access-lists**

# show access-lists

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

**show access-lists [name | number | hardware counters | ipc]**

## Syntax Description

<i>name</i>	(Optional) Name of the ACL.
<i>number</i>	(Optional) ACL number. The range is 1 to 2699.
<b>hardware counters</b>	(Optional) Display global hardware ACL statistics for switched and routed packets.
<b>ipc</b>	(Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information.
<i>expression</i>	Expression in the output to use as a reference point.

## Command Modes

Privileged EXEC

## Command History

### Usage Guidelines

The switch supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2699.

This command also displays the MAC ACLs that are configured.



### Note

Though visible in the command-line help strings, the **rate-limit** keywords are not supported.

**Examples**

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 1
 10 permit 1.1.1.1
 20 permit 2.2.2.2
 30 permit any
 40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
 10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
 10 permit 10.10.10.10
Extended IP access list 121
 10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
Extended IP access list CMP-NAT-ACL
  Dynamic Cluster-HSRP deny ip any any
 10 deny ip any host 19.19.11.11
 20 deny ip any host 10.11.12.13
  Dynamic Cluster-NAT permit ip any any any
 10 permit ip host 10.99.100.128 any
 20 permit ip host 10.46.22.128 any
 30 permit ip host 10.45.101.64 any
 40 permit ip host 10.45.20.64 any
 50 permit ip host 10.213.43.128 any
 60 permit ip host 10.91.28.64 any
 70 permit ip host 10.99.75.128 any
 80 permit ip host 10.38.49.0 any
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
  Drop:           All frame count: 855
  Drop:           All bytes count: 94143
  Drop And Log:  All frame count: 0
  Drop And Log:  All bytes count: 0
  Bridge Only:   All frame count: 0
  Bridge Only:   All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU: All frame count: 0
  Forwarding To CPU: All bytes count: 0
  Forwarded:     All frame count: 2121
  Forwarded:     All bytes count: 180762
  Forwarded And Log: All frame count: 0
  Forwarded And Log: All bytes count: 0

L3 ACL INPUT Statistics
  Drop:           All frame count: 0
  Drop:           All bytes count: 0
  Drop And Log:  All frame count: 0
  Drop And Log:  All bytes count: 0
  Bridge Only:   All frame count: 0
  Bridge Only:   All bytes count: 0
  Bridge Only And Log: All frame count: 0
  Bridge Only And Log: All bytes count: 0
  Forwarding To CPU: All frame count: 0
  Forwarding To CPU: All bytes count: 0
  Forwarded:     All frame count: 13586
  Forwarded:     All bytes count: 1236182
  Forwarded And Log: All frame count: 0
  Forwarded And Log: All bytes count: 0
```

■ **show access-lists**

```
L2 ACL OUTPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 232983
Forwarded: All bytes count: 16825661
Forwarded And Log: All frame count: 0
Forwarded And Log: All bytes count: 0

L3 ACL OUTPUT Statistics
Drop: All frame count: 0
Drop: All bytes count: 0
Drop And Log: All frame count: 0
Drop And Log: All bytes count: 0
Bridge Only: All frame count: 0
Bridge Only: All bytes count: 0
Bridge Only And Log: All frame count: 0
Bridge Only And Log: All bytes count: 0
Forwarding To CPU: All frame count: 0
Forwarding To CPU: All bytes count: 0
Forwarded: All frame count: 514434
Forwarded: All bytes count: 39048748
Forwarded And Log: All frame count: 0
Forwarded And Log: All bytes count: 0
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>access-list</b>	Configures a standard or extended numbered access list on the switch.
<b>ip access list</b>	Configures a named IP access list on the switch.
<b>mac access-list extended</b>	Configures a named or numbered MAC access list on the switch.

# show archive status

Use the **show archive status** privileged EXEC command to display the status of a new image being downloaded to a switch with the HTTP or the TFTP protocol.

## show archive status

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

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** If you use the **archive download-sw** privileged EXEC command to download an image to a TFTP server, the output of the **archive download-sw** command shows the status of the download.

If you do not have a TFTP server, you can use Network Assistant or the embedded device manager to download the image by using HTTP. The **show archive status** command shows the progress of the download.

## Examples

These are examples of output from the **show archive status** command:

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

## Related Commands

Command	Description
<a href="#">archive download-sw</a>	Downloads a new image from a TFTP server to the switch.

---

 show arp access-list
 

---

## show arp access-list

Use the **show arp access-list** EXEC command to display detailed information about Address Resolution Protocol (ARP) access control (lists).

**show arp access-list [acl-name]**

<b>Syntax Description</b>	<i>acl-name</i> (Optional) Name of the ACL.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	
------------------------	--

<b>Examples</b>	This is an example of output from the <b>show arp access-list</b> command:
-----------------	--

```
Switch# show arp access-list
ARP access list rose
  permit ip 10.101.1.1 0.0.0.255 mac any
  permit ip 20.3.1.0 0.0.0.255 mac any
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">arp access-list</a>	Defines an ARP ACL.
	<a href="#">deny (ARP access-list configuration)</a>	Denies an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings.
	<a href="#">ip arp inspection filter vlan</a>	Permits ARP requests and responses from a host configured with a static IP address.
	<a href="#">permit (ARP access-list configuration)</a>	Permits an ARP packet based on matches against the DHCP bindings.

# show authentication

Use the **show authentication** EXEC command to display information about authentication manager events on the switch.

```
show authentication {interface interface-id | registrations | sessions [session-id session-id]
[handle handle] [interface interface-id] [mac mac] [method method] | statistics [summary]}
```

Syntax Description		
<b>interface interface-id</b>	(Optional)	Display all of the authentication manager details for the specified interface.
<b>method method</b>	(Optional)	Displays all clients authorized by a specified authentication method ( <b>dot1x</b> , <b>mab</b> , or <b>webauth</b> )
<b>registrations</b>	(Optional)	Display authentication manager registrations
<b>sessions</b>	(Optional)	Display detail of the current authentication manager sessions (for example, client devices). If you do not enter any optional specifiers, all current active sessions are displayed. You can enter the specifiers singly or in combination to display a specific session (or group of sessions).
<b>session-id session-id</b>	(Optional)	Specify an authentication manager session.
<b>handle handle</b>	(Optional)	Specify a range from 1 to 4294967295.
<b>mac mac</b>	(Optional)	Display authentication manager information for a specified MAC address.
<b>statistics</b>	(Optional)	Display authentication statistics in detail.
<b>summary</b>	(Optional)	Display authentication statistics summary.

**Command Default** This command has no default settings.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** Table 2-25 describes the significant fields shown in the output of the **show authentication** command.



The possible values for the status of sessions are shown below. For a session in terminal state, *Authz Success* or *Authz Failed* is displayed along with *No methods* if no method has provided a result.

■ **show authentication**

**Table 0-1 show authentication Command Output**

Field	Description
Idle	The session has been initialized and no methods have run yet.
Running	A method is running for this session.
No methods	No method has provided a result for this session.
Authc Success	A method has resulted in authentication success for this session.
Authc Failed	A method has resulted in authentication fail for this session.
Authz Success	All features have been successfully applied for this session.
Authz Failed	A feature has failed to be applied for this session.

**Table 2-26** lists the possible values for the state of methods. For a session in a terminal state, *Authc Success*, *Authc Failed*, or *Failed over* are displayed. *Failed over* means that an authentication method ran and then failed over to the next method, which did not provide a result. *Not run* appears for sessions that synchronized on standby.

**Table 0-2 State Method Values**

Method State	State Level	Description
Not run	Terminal	The method has not run for this session.
Running	Intermediate	The method is running for this session.
Failed over	Terminal	The method has failed and the next method is expected to provide a result.
Authc Success	Terminal	The method has provided a successful authentication result for the session.
Authc Failed	Terminal	The method has provided a failed authentication result for the session.

## Examples

This is an example the **show authentication registrations** command:

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
Handle Priority Name
3 0 dot1x
2 1 mab
1 2 webauth
```

This is an example of the **show authentication interface interface-id** command:

```
Client list:
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000
Available methods list:
Handle Priority Name
3 0 dot1x
Runnable methods list:
Handle Priority Name
3 0 dot1x
```

This is an example of the **show authentication sessions** command:

```
Switch# show authentication sessions
Interface  MAC Address      Method   Domain    Status        Session ID
Gi3/45     (unknown)       N/A      DATA      Authz Failed  0908140400000007003651EC
Gi3/46     (unknown)       N/A      DATA      Authz Success 09081404000000080057C274
```

This is an example of the **show authentication sessions** command for a specified interface:

```
Interface:
  MAC Address: Unknown
  IP Address: Unknown
  Status: Authz Success
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Authorized By: Guest Vlan
  Vlan Policy: 4094
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 09081404000000080057C274
  Acct Session ID: 0x0000000A
  Handle: 0xCC000008
Runnable methods list:
  Method  State
  dot1x   Failed over
```

This is an example of the **show authentication sessions** command for a specified MAC address:

```
Switch# show authentication sessions mac 000e.84af.59bd
Interface:
MAC Address: 000e.84af.59bd
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

This is an example of the **show authentication session method** command for a specified method:

```
Switch# show authentication sessions method mab
No Auth Manager contexts match supplied criteria
Switch# show authentication sessions method dot1x
MAC Address Domain Status Handle Interface
000e.84af.59bd DATA Authz Success 0xE0000000 GigabitEthernet1/23
```

## Related Commands

Command	Description
<a href="#">authentication control-direction</a>	Configures the port mode as unidirectional or bidirectional.
<a href="#">authentication event</a>	Sets the action for specific authentication events.
<a href="#">authentication event linksec fail action</a>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
<a href="#">authentication host-mode</a>	Sets the authorization manager mode on a port.
<a href="#">authentication open</a>	Enables or disables open access on a port.

**show authentication**

Command	Description
<b>authentication order</b>	Sets the order of authentication methods used on a port.
<b>authentication periodic</b>	Enables or disables reauthentication on a port.
<b>authentication port-control</b>	Enables manual control of the port authorization state.
<b>authentication priority</b>	Adds an authentication method to the port-priority list.
<b>authentication timer</b>	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.

# show auto qos

To display the quality of service (QoS) commands entered on the interfaces on which automatic QoS (auto-QoS) is enabled, use the **show auto qos** command in EXEC mode.

**show auto qos [interface [interface-id]]**

<b>Syntax Description</b>	<b>interface [interface-id]</b>	(Optional) Display auto-QoS information for the specified port or for all ports. Valid interfaces include physical ports.
---------------------------	---------------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(40)SE	The information in the command output changed.

**Usage Guidelines** The **show auto qos** command output shows only the auto-QoS command entered on each interface. The **show auto qos interface interface-id** command output shows the auto-QoS command entered on a specific interface.

Use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

The **show auto qos** command output also shows the service policy information for the Cisco IP phone.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface [interface-id] [buffers | queueing]**
- **show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]**
- **show mls qos input-queue**
- **show running-config**

■ **show auto qos**

## Examples

This is an example of output from the **show auto qos** command after the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show auto qos
GigabitEthernet0/4
auto qos voip cisco-softphone

GigabitEthernet0/5
auto qos voip cisco-phone

GigabitEthernet0/6
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface interface-id** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet 0/5
GigabitEthernet0/5
auto qos voip cisco-phone
```

This is an example of output from the **show running-config** privileged EXEC command when the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show running-config
Building configuration...
...
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 100 100 100 100
```

```

mls qos queue-set output 1 threshold 2 75 75 75 250
mls qos queue-set output 1 threshold 3 75 150 100 300
mls qos queue-set output 1 threshold 4 50 100 75 400
mls qos queue-set output 2 threshold 1 100 100 100 100
mls qos queue-set output 2 threshold 2 35 35 35 35
mls qos queue-set output 2 threshold 3 55 82 100 182
mls qos queue-set output 2 threshold 4 90 250 100 400
mls qos queue-set output 1 buffers 15 20 20 45
mls qos queue-set output 2 buffers 24 20 26 30
mls qos
...
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp ef
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3 af31
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
!
policy-map AutoQoS-Police-CiscoPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp ef
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp cs3
    police 32000 8000 exceed-action policed-dscp-transmit
...
!
switchport mode access
switchport port-security maximum 400
service-policy input AutoQoS-Police-SoftPhone
speed 100
duplex half
srr-queue bandwidth share 10 10 60 20
priority-queue out
auto qos voip cisco-softphone
!
interface GigabitEthernet0/5
switchport mode access
switchport port-security maximum 1999
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
!
interface GigabitEthernet0/6
switchport trunk encapsulation dot1q
switchport trunk native vlan 2
switchport mode access
speed 10
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone

```

■ **show auto qos**

```
!
interface GigabitEthernet0/1
srr-queue bandwidth share 10 10 60 20
priority-queue out
mls qos trust device cisco-phone
mls qos trust cos
mls qos trust device cisco-phone
service-policy input AutoQoS-Police-CiscoPhone
```

<output truncated>

This is an example of output from the **show auto qos interface *interface-id*** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface Gigabitethernet0/2
auto qos voip cisco-softphone
```

This is an example of output from the **show auto qos** command when auto-QoS is disabled on the switch:

```
Switch# show auto qos
AutoQoS not enabled on any interface
```

This is an example of output from the **show auto qos interface *interface-id*** command when auto-QoS is disabled on an interface:

```
Switch# show auto qos interface gigabitethernet0/1
AutoQoS is disabled
```

#### Related Commands

Command	Description
<a href="#">auto qos voip</a>	Automatically configures QoS for VoIP within a QoS domain.
<a href="#">debug auto qos</a>	Enables debugging of the auto-QoS feature.

# show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

## show boot

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

**Command Modes** Privileged EXEC

## Command History

**Examples** This is an example of output from the **show boot** command. [Table 2-27](#) describes each field in the display.

```
Switch# show boot
BOOT path-list      :flash:/image
Config file        :flash:/config.text
Private Config file :flash:/private-config.text
Enable Break       :no
Manual Boot        :yes
HELPER path-list   :
Auto upgrade       :yes
-----
```

**Table 0-3** *show boot Field Descriptions*

Field	Description
BOOT path-list	Displays a semicolon separated list of executable files to try to load and execute when automatically booting up.  If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.  If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot up with the first bootable file that it can find in the flash file system.
Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting up is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic bootup process by pressing the Break key on the console after the flash file system is initialized.

**show boot****Table 0-3** *show boot Field Descriptions*

Field	Description
Manual Boot	Displays whether the switch automatically or manually boots up. If it is set to no or 0, the bootloader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the bootloader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the bootloader initialization. Helper files extend or patch the functionality of the bootloader.

**Related Commands**

Command	Description
<a href="#"><b>boot config-file</b></a>	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
<a href="#"><b>boot enable-break</b></a>	Enables interrupting the automatic boot process.
<a href="#"><b>boot manual</b></a>	Enables manually booting up the switch during the next bootup cycle.
<a href="#"><b>boot private-config-file</b></a>	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
<a href="#"><b>boot system</b></a>	Specifies the Cisco IOS image to load during the next bootup cycle.

# show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** privileged EXEC command to display the Time Domain Reflector (TDR) results.

**show cable-diagnostics tdr interface *interface-id***

<b>Syntax Description</b>	<i>interface-id</i> Specify the interface on which TDR was run.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

For more information about TDR, see the software configuration guide for this release.

**Examples** This is an example of output from the **show cable-diagnostics tdr interface *interface-id*** command:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length      Remote pair Pair status
-----  -----
Gi0/2    auto   Pair A    0    +/- 2 meters N/A        Open
                  Pair B    0    +/- 2 meters N/A        Open
                  Pair C    0    +/- 2 meters N/A        Open
                  Pair D    0    +/- 2 meters N/A        Open
```

Table 2-28 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

**Table 0-4 Fields Descriptions for the show cable-diagnostics tdr Command Output**

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> <li>• The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s.</li> <li>• The cable is open.</li> <li>• The cable has a short.</li> </ul>

---

```
show cable-diagnostics tdr
```

---

**Table 0-4 Fields Descriptions for the show cable-diagnostics tdr Command Output (continued)**

Field	Description
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: <ul style="list-style-type: none"> <li>• Normal—The pair of wires is properly connected.</li> <li>• Not completed—The test is running and is not completed.</li> <li>• Not supported—The interface does not support TDR.</li> <li>• Open—The pair of wires is open.</li> <li>• Shorted—The pair of wires is shorted.</li> <li>• ImpedanceMis—The impedance is mismatched.</li> <li>• Short/Impedance Mismatched—The impedance mismatched or the cable is short.</li> <li>• InProgress—The diagnostic test is in progress</li> </ul>

This is an example of output from the **show interfaces interface-id** command when TDR is running:

```
gigabitethernet0/2 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostic tdr interface interface-id** command when TDR is not running:

```
Switch# show cable-diagnostic tdr interface
% TDR test was never issued on Gi0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on switch 1
```

#### Related Commands

Command	Description
<a href="#">test cable-diagnostic tdr</a>	Enables and runs TDR on an interface.

# show cisp

Use the **show cisp** privileged EXEC command to display CISP information for a specified interface.

**show cisp {[interface *interface-id*] | clients | summary}**

Syntax Description	<b>clients</b> (Optional) Display CISP client details
<b>interface <i>interface-id</i></b>	(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
<b>summary</b>	(Optional) Display
<b>expression</b>	Expression in the output to use as a reference point.

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

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

<b>Examples</b>	This example shows output from the <b>show cisp interface</b> command:
	WS-C3750E-48TD#show cisp interface fast 0 CISP not enabled on specified interface

This example shows output from the **show cisp summary** command:

CISP is not running on any interface

Related Commands	Command	Description
	<b>dot1x credentials profile</b>	Configure a profile on a supplicant switch
	<b>cisp enable</b>	Enable Client Information Signalling Protocol (CISP)

**show class-map**

# show class-map

Use the **show class-map** EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

**show class-map [class-map-name]**

<b>Syntax Description</b>	<i>class-map-name</i> (Optional) Display the contents of the specified class map.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	
------------------------	--

<b>Examples</b>	This is an example of output from the <b>show class-map</b> command:
-----------------	--

```
Switch# show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10

  Class Map match-any class-default (id 0)
    Match any
  Class Map match-all dscp5 (id 3)
    Match ip dscp 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>class-map</b></a>	Creates a class map to be used for matching packets to the class whose name you specify.
	<a href="#"><b>match (class-map configuration)</b></a>	Defines the match criteria to classify traffic.

# show cluster

Use the **show cluster** EXEC command to display the cluster status and a summary of the cluster to which the switch belongs. This command can be entered on the cluster command switch and cluster member switches.

## show cluster

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Usage Guidelines** If you enter this command on a switch that is not a cluster member, the error message `Not a management cluster member` appears.

On a cluster member switch, this command displays the identity of the cluster command switch, the switch member number, and the state of its connectivity with the cluster command switch.

On a cluster command switch, this command displays the cluster name and the total number of members. It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.

## Examples

This is an example of output when the **show cluster** command is entered on the cluster command switch:

```
Switch# show cluster
Command switch for cluster "Ajang"
    Total number of members: 7
    Status: 1 members are unreachable
    Time since last status change: 0 days, 0 hours, 2 minutes
    Redundancy: Enabled
        Standby command switch: Member 1
        Standby Group: Ajang_standby
        Standby Group Number: 110
        Heartbeat interval: 8
        Heartbeat hold-time: 80
        Extended discovery hop count: 3
```

This is an example of output when the **show cluster** command is entered on a cluster member switch:

```
Switch1> show cluster
Member switch for cluster "hapuna"
    Member number: 3
    Management IP address: 192.192.192.192
    Command switch mac address: 0000.0c07.ac14
    Heartbeat interval: 8
    Heartbeat hold-time: 80
```

This is an example of output when the **show cluster** command is entered on a cluster member switch that is configured as the standby cluster command switch:

```
Switch# show cluster
```

**show cluster**

```
Member switch for cluster "hapuna"
  Member number:           3 (Standby command switch)
  Management IP address: 192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:      8
  Heartbeat hold-time:     80
```

This is an example of output when the **show cluster** command is entered on the cluster command switch that has lost connectivity with member 1:

```
Switch# show cluster
Command switch for cluster "Ajang"
  Total number of members:    7
  Status:                   1 members are unreachable
  Time since last status change: 0 days, 0 hours, 5 minutes
  Redundancy:                Disabled
  Heartbeat interval:        8
  Heartbeat hold-time:       80
  Extended discovery hop count: 3
```

This is an example of output when the **show cluster** command is entered on a cluster member switch that has lost connectivity with the cluster command switch:

```
Switch# show cluster
Member switch for cluster "hapuna"
  Member number:           <UNKNOWN>
  Management IP address: 192.192.192.192
  Command switch mac address: 0000.0c07.ac14
  Heartbeat interval:      8
  Heartbeat hold-time:     80
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>cluster enable</b></a>	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
<a href="#"><b>show cluster candidates</b></a>	Displays a list of candidate switches.
<a href="#"><b>show cluster members</b></a>	Displays information about the cluster members.

# show cluster candidates

Use the **show cluster candidates** EXEC command to display a list of candidate switches.

**show cluster candidates [detail | mac-address H.H.H.]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed information for all candidates. <b>mac-address H.H.H.</b> (Optional) MAC address of the cluster candidate.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Usage Guidelines

This command is available only on the cluster command switch.

If the switch is not a cluster command switch, the command displays an empty line at the prompt.

The SN in the display means *switch member number*. If E appears in the SN column, it means that the switch is discovered through extended discovery. If E does not appear in the SN column, it means that the *switch member number* is the upstream neighbor of the candidate switch. The hop count is the number of devices the candidate is from the cluster command switch.

### Examples

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

```
Switch# show cluster candidates
|---Upstream---|
MAC Address      Name       Device Type    PortIf   FEC Hops  SN PortIf   FEC
00d0.7961.c4c0  StLouis-2  WS-C12T     Gi0/1    2   1     Fa0/11
00d0.bbf5.e900  ldf-dist-128 WS-C3524-XL  Fa0/7    1   0     Fa0/24
00e0.1e7e.be80  1900_Switch 1900        3        0   1     Fa0/11
00e0.1e9f.7a00  Surfers-24  WS-C2924-XL  Fa0/5    1   0     Fa0/3
00e0.1e9f.8c00  Surfers-12-2 WS-C2912-XL  Fa0/4    1   0     Fa0/7
00e0.1e9f.8c40  Surfers-12-1 WS-C2912-XL  Fa0/1    1   0     Fa0/9
```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a cluster member switch directly connected to the cluster command switch:

```
Switch# show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
  Device type:          cisco WS-C12T
  Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
  Local port:           Gi0/1   FEC number:
  Upstream port:        Gi0/11  FEC Number:
  Hops from cluster edge: 1
  Hops from command device: 1
```

This is an example of output from the **show cluster candidates** command that uses the MAC address of a cluster member switch three hops from the cluster edge:

```
Switch# show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
  Device type:          cisco WS-C2912MF-XL
```

**show cluster candidates**

```

Upstream MAC address: 0010.7bb6.1cd4
Local port: Fa2/1 FEC number:
Upstream port: Fa0/24 FEC Number:
Hops from cluster edge: 3
Hops from command device: -

```

This is an example of output from the **show cluster candidates detail** command:

```

Switch# show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
    Device type: cisco WS-C3512-XL
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 1)
    Local port: Fa0/3 FEC number:
    Upstream port: Fa0/13 FEC Number:
    Hops from cluster edge: 1
    Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
    Device type: cisco 1900
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 2)
    Local port: 3 FEC number: 0
    Upstream port: Fa0/11 FEC Number:
    Hops from cluster edge: 1
    Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
    Device type: cisco WS-C2924-XL
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 3)
    Local port: Fa0/5 FEC number:
    Upstream port: Fa0/3 FEC Number:
    Hops from cluster edge: 1
    Hops from command device: 2

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show cluster</b></a>	Displays the cluster status and a summary of the cluster to which the switch belongs.
<a href="#"><b>show cluster members</b></a>	Displays information about the cluster members.

# show cluster members

Use the **show cluster members** privileged EXEC command to display information about the cluster members.

**show cluster members [n | detail]**

## Syntax Description

<b>n</b>	(Optional) Number that identifies a cluster member. The range is 0 to 15.
<b>detail</b>	(Optional) Display detailed information for all cluster members.

## Command Modes

Privileged EXEC

## Command History

### Usage Guidelines

This command is available only on the cluster command switch.

If the cluster has no members, this command displays an empty line at the prompt.

## Examples

This is an example of output from the **show cluster members** command. The SN in the display means *switch number*.

```
Switch# show cluster members
      |---Upstream---|
SN MAC Address     Name       PortIf FEC Hops   SN PortIf   FEC State
0  0002.4b29.2e00  StLouis1        0          Up    (Cmdr)
1  0030.946c.d740  tal-switch-1  Fa0/13    1      0  Gi0/1      Up
2  0002.b922.7180  nms-2820    10      0  2      1  Fa0/18      Up
3  0002.4b29.4400  SanJuan2     Gi0/1     2      1  Fa0/11      Up
4  0002.4b28.c480  GenieTest   Gi0/2     2      1  Fa0/9       Up
```

This is an example of output from the **show cluster members** for cluster member 3:

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
  Device type:           cisco WS-C
  MAC address:          0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port:            Gi0/1   FEC number:
  Upstream port:         GI0/11  FEC Number:
  Hops from command device: 2
```

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

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
  Device type:           cisco WS-C
  MAC address:          0002.4b29.2e00
  Upstream MAC address:
  Local port:            FEC number:
  Upstream port:         FEC Number:
  Hops from command device: 0
Device 'tal-switch-14' with member number 1
  Device type:           cisco WS-C3548-XL
  MAC address:          0030.946c.d740
```

**show cluster members**

```

Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
Local port: Fa0/13 FEC number:
Upstream port: Gi0/1 FEC Number:
Hops from command device: 1
Device 'nms-2820' with member number 2
  Device type: cisco 2820
  MAC address: 0002.b922.7180
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port: 10 FEC number: 0
  Upstream port: Fa0/18 FEC Number:
  Hops from command device: 2
Device 'SanJuan2' with member number 3
  Device type: cisco WS-C
  MAC address: 0002.4b29.4400
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port: Gi0/1 FEC number:
  Upstream port: Fa0/11 FEC Number:
  Hops from command device: 2
Device 'GenieTest' with member number 4
  Device type: cisco SeaHorse
  MAC address: 0002.4b28.c480
  Upstream MAC address: 0030.946c.d740 (Cluster member 1)
  Local port: Gi0/2 FEC number:
  Upstream port: Fa0/9 FEC Number:
  Hops from command device: 2
Device 'Palpatine' with member number 5
  Device type: cisco WS-C2924M-XL
  MAC address: 00b0.6404.f8c0
  Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
  Local port: Gi2/1 FEC number:
  Upstream port: Gi0/7 FEC Number:
  Hops from command device: 1

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show cluster</b></a>	Displays the cluster status and a summary of the cluster to which the switch belongs.
<a href="#"><b>show cluster candidates</b></a>	Displays a list of candidate switches.

# show controllers cpu-interface

Use the **show controllers cpu-interface** privileged EXEC command to display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU.

## show controllers cpu-interface

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

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

## Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface
cpu-queue-frames retrieved dropped invalid hol-block
----- -----
rpc          4523063   0      0      0
stp          1545035   0      0      0
ipc          1903047   0      0      0
routing protocol 96145   0      0      0
L2 protocol    79596   0      0      0
remote console  0      0      0      0
sw forwarding   5756    0      0      0
host          225646   0      0      0
broadcast      46472   0      0      0
cbt-to-spt     0      0      0      0
igmp snooping  68411   0      0      0
icmp          0      0      0      0
logging         0      0      0      0
rpf-fail        0      0      0      0
queue14        0      0      0      0
cpu heartbeat   1710501  0      0      0

Supervisor ASIC receive-queue parameters
-----
queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
queue 3 maxrecevsize 5EE pakhead 19CDDDO paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----
MicDirectPollInfo           80000800
MicIndicationsReceived      00000000
MicInterruptsReceived       00000000
MicPcsInfo                  0001001F
MicPlbMasterConfiguration   00000000
```

**show controllers cpu-interface**

```

MicRxFifosAvailable          00000000
MicRxFifosReady              0000BFFF
MicTimeOutPeriod:           FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0: StartPtrs: 038C2800     ReadPtr: 038C2C38
      WritePtrs: 038C2C38      Fifo_Flag: 8A800800
      Weights: 001E001E
Fifo1: StartPtr: 03A9BC00     ReadPtr: 03A9BC60
      WritePtrs: 03A9BC60      Fifo_Flag: 89800400
      writeHeaderPtr: 03A9BC60
Fifo2: StartPtr: 038C8800     ReadPtr: 038C88E0
      WritePtrs: 038C88E0      Fifo_Flag: 88800200
      writeHeaderPtr: 038C88E0
Fifo3: StartPtr: 03C30400     ReadPtr: 03C30638
      WritePtrs: 03C30638      Fifo_Flag: 89800400
      writeHeaderPtr: 03C30638
Fifo4: StartPtr: 03AD5000     ReadPtr: 03AD50A0
      WritePtrs: 03AD50A0      Fifo_Flag: 89800400
      writeHeaderPtr: 03AD50A0
Fifo5: StartPtr: 03A7A600     ReadPtr: 03A7A600
      WritePtrs: 03A7A600      Fifo_Flag: 88800200
      writeHeaderPtr: 03A7A600
Fifo6: StartPtr: 03BF8400     ReadPtr: 03BF87F0
      WritePtrs: 03BF87F0      Fifo_Flag: 89800400

<output truncated>

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show controllers ethernet-controller</b>	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
<b>show interfaces</b>	Displays the administrative and operational status of all interfaces or a specified interface.

# show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-interface send and receive statistics read from the hardware. Use with the **phy** keyword to display the interface internal registers or the **port-asic** keyword to display information about the port ASIC.

```
show controllers ethernet-controller [interface-id] [phy [detail]] [port-asic {configuration | statistics}] [fastethernet 0]
```

Syntax Description	
<i>interface-id</i>	The physical interface (including type, module, and port number).
<b>phy</b>	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface.
<b>detail</b>	(Optional) Display details about the PHY internal registers.
<b>port-asic</b>	(Optional) Display information about the port ASIC internal registers.
<b>configuration</b>	Display port ASIC internal register configuration.
<b>statistics</b>	Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.

**Command Modes** Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

## Command History

## Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for all interfaces or for the specified interface.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

## Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-29 lists the *Transmit* fields, and Table 2-30 lists the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1                                Receive
      0 Bytes                                         0 Bytes
      0 Unicast frames                               0 Unicast frames
      0 Multicast frames                            0 Multicast frames
      0 Broadcast frames                           0 Broadcast frames
      0 Too old frames                             0 Unicast bytes
      0 Deferred frames                           0 Multicast bytes
      0 MTU exceeded frames                      0 Broadcast bytes
      0 1 collision frames                        0 Alignment errors
      0 2 collision frames                        0 FCS errors
      0 3 collision frames                        0 Oversize frames
      0 4 collision frames                        0 Undersize frames
      0 5 collision frames                        0 Collision fragments
      0 6 collision frames
      0 7 collision frames
      0 8 collision frames
                                         0 Minimum size frames
                                         0 65 to 127 byte frames
```

```
■ show controllers ethernet-controller
```

0 9 collision frames	0 128 to 255 byte frames
0 10 collision frames	0 256 to 511 byte frames
0 11 collision frames	0 512 to 1023 byte frames
0 12 collision frames	0 1024 to 1518 byte frames
0 13 collision frames	0 Overrun frames
0 14 collision frames	0 Pause frames
0 15 collision frames	0 Symbol error frames
0 Excessive collisions	
0 Late collisions	0 Invalid frames, too large
0 VLAN discard frames	0 Valid frames, too large
0 Excess defer frames	0 Invalid frames, too small
0 64 byte frames	0 Valid frames, too small
0 127 byte frames	
0 255 byte frames	0 Too old frames
0 511 byte frames	0 Valid oversize frames
0 1023 byte frames	0 System FCS error frames
0 1518 byte frames	0 RxPortFifoFull drop frame
0 Too large frames	
0 Good (1 coll) frames	

**Table 0-5      Transmit Field Descriptions**

Field	Description
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.

**Table 0-5** *Transmit Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI <sup>1</sup> bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames sent on an interface that are 64 bytes.
127 byte frames	The total number of frames sent on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames sent on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames sent on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames sent on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames sent on an interface that are from 1024 to 1518 bytes.
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.

1. CFI = Canonical Format Indicator

**Table 0-6** *Receive Field Descriptions*

<b>Field</b>	<b>Description</b>
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.

■ **show controllers ethernet-controller**

**Table 0-6      Receive Field Descriptions (continued)**

Field	Description
Collision fragments	The number of collision fragments received on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too large	The number of frames received on an interface that are larger than the maximum allowed frame size.
Invalid frames, too small	The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too small	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Too old frames	The number of frames dropped on the ingress port because the packet aged out.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.
System FCS error frames	The total number of frames received on an interface that have a valid length (in bytes) but that do not have the correct FCS values.
RxPortFifoFull drop frames	The total number of frames received on an interface that are dropped because the ingress queue is full.

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface:

This is an example of output from the **show controllers ethernet-controller port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration
=====
Switch 1, PortASIC 0 Registers
-----
DeviceType : 000101BC
Reset : 00000000
PmadMicConfig : 00000001
PmadMicDiag : 00000003
SupervisorReceiveFifoSramInfo : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo : 000001D0 000001D0 40000000
GlobalStatus : 00000800
```

```

IndicationStatus : 00000000
IndicationStatusMask : FFFFFFFF
InterruptStatus : 00000000
InterruptStatusMask : 01FFE800
SupervisorDiag : 00000000
SupervisorFrameSizeLimit : 000007C8
SupervisorBroadcast : 000A0F01
GeneralIO : 000003F9 00000000 00000004
StackPcsInfo : FFFF1000 860329BD 5555FFFF FFFFFFFF
FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo : 73001630 00000003 7F001644 00000003
24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus : 18E418E0
stackControlStatusMask : FFFFFFFF
TransmitBufferFreeListInfo : 00000854 00000800 00000FF8 00000000
0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo : 00000016 00000016 40000000 00000000
0000000C 0000000C 40000000 00000000
TransmitBufferInfo : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount : 00000F7A
TransmitBufferCommonCountPeak : 0000001E
TransmitBufferCommonCommonEmpty : 000000FF
NetworkActivity : 00000000 00000000 00000000 02400000
DroppedStatistics : 00000000
FrameLengthDeltaSelect : 00000001
SneakPortFifoInfo : 00000000
MacInfo : 0EC0801C 00000001 0EC0801B 00000001
00C0001D 00000001 00C0001E 00000001

```

<output truncated>

This is an example of output from the **show controllers ethernet-controller port-asic statistics** command:

```

Switch# show controllers ethernet-controller port-asic statistics
=====
Switch 1, PortASIC 0 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames          0 RxQ-0, wt-0 drop frames
4118966 RxQ-0, wt-1 enqueue frames       0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames          0 RxQ-0, wt-2 drop frames

      0 RxQ-1, wt-0 enqueue frames          0 RxQ-1, wt-0 drop frames
      296 RxQ-1, wt-1 enqueue frames        0 RxQ-1, wt-1 drop frames
2836036 RxQ-1, wt-2 enqueue frames       0 RxQ-1, wt-2 drop frames

      0 RxQ-2, wt-0 enqueue frames          0 RxQ-2, wt-0 drop frames
      0 RxQ-2, wt-1 enqueue frames          0 RxQ-2, wt-1 drop frames
158377 RxQ-2, wt-2 enqueue frames        0 RxQ-2, wt-2 drop frames

      0 RxQ-3, wt-0 enqueue frames          0 RxQ-3, wt-0 drop frames
      0 RxQ-3, wt-1 enqueue frames          0 RxQ-3, wt-1 drop frames
      0 RxQ-3, wt-2 enqueue frames          0 RxQ-3, wt-2 drop frames

      15 TxBUFFERFull Drop Count           0 Rx Fcs Error Frames
      0 TxBUFFERFrameDesc BadCrc16         0 Rx Invalid Oversize Frames
      0 TxBUFFER Bandwidth Drop Cou        0 Rx Invalid Too Large Frames
      0 TxQueue Bandwidth Drop COUN        0 Rx Invalid Too Large Frames
      0 TxQueue Missed Drop Statist       0 Rx Invalid Too Small Frames
      74 TxBUFFER Drop DestIndex Cou       0 Rx Too Old Frames
      0 SneakQueue Drop Count             0 Tx Too Old Frames
      0 Learning Queue Overflow Fra       0 System Fcs Error Frames
      0 Learning Cam Skip Count

```

```
■ show controllers ethernet-controller
```

```
15 Sup Queue 0 Drop Frames          0 Sup Queue 8 Drop Frames
 0 Sup Queue 1 Drop Frames          0 Sup Queue 9 Drop Frames
 0 Sup Queue 2 Drop Frames          0 Sup Queue 10 Drop Frames
 0 Sup Queue 3 Drop Frames          0 Sup Queue 11 Drop Frames
 0 Sup Queue 4 Drop Frames          0 Sup Queue 12 Drop Frames
 0 Sup Queue 5 Drop Frames          0 Sup Queue 13 Drop Frames
 0 Sup Queue 6 Drop Frames          0 Sup Queue 14 Drop Frames
 0 Sup Queue 7 Drop Frames          0 Sup Queue 15 Drop Frames
=====
=====
=====
```

```
Switch 1, PortASIC 1 Statistics
-----
      0 RxQ-0, wt-0 enqueue frames      0 RxQ-0, wt-0 drop frames
      52 RxQ-0, wt-1 enqueue frames     0 RxQ-0, wt-1 drop frames
      0 RxQ-0, wt-2 enqueue frames     0 RxQ-0, wt-2 drop frames

<output truncated>
```

**Related Commands**

Command	Description
<a href="#"><b>show controllers cpu-interface</b></a>	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
<a href="#"><b>show controllers team</b></a>	Displays the state of registers for all ternary content addressable memory (TCAM) in the system and for TCAM interface ASICs that are CAM controllers.

---

■ show controllers power inline

## show controllers power inline

Use the **show controllers power inline** command in EXEC mode to display the values in the registers of the specified Power over Ethernet (PoE) controller.

**show controllers power inline [instance]**

<b>Syntax Description</b>	<i>instance</i>  (Optional) Power controller instance, where each instance corresponds to four ports. See the “Usage Guidelines” section for more information. If no instance is specified, information for all instances appear.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

### Command History

#### Usage Guidelines

Though visible on all switches, this command is valid only for PoE switches. It provides no information for switches that do not support PoE.

The output provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

**Examples**

This is an example of output from the **show controllers power inline** command on a Catalyst switch:

```
Switch# show controllers power inline
Alchemy instance 0, address 0
Pending event flag      :N N N N N N N N N N N N N N N N
Current State           :00 05 10 51 61 11
Current Event            :00 01 00 10 40 00
Timers                  :00 C5 57 03 12 20 04 B2 05 06 07 07
Error State              :00 00 00 00 10 00
Error Code                :00 00 00 00 00 00 00 00 00 00 00 00
Power Status             :N Y N N Y N N N N N N N N N N
Auto Config              :N Y Y N Y Y Y Y Y Y Y Y
Disconnect               :N N N N N N N N N N N N N N N N
Detection Status         :00 00 00 30 00 00
Current Class             :00 00 00 30 00 00
Tweetie debug             :00 00 00 00
POE Commands pending at sub:
    Command 0 on each port :00 00 00 00 00 00 00 00
    Command 1 on each port :00 00 00 00 00 00 00 00
    Command 2 on each port :00 00 00 00 00 00 00 00
    Command 3 on each port :00 00 00 00 00 00 00 00
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">logging event</a>	Enables the logging of PoE events.
<a href="#">power-inline-status</a>	
<a href="#">power inline</a>	Configures the power management mode for the specified PoE port or for all PoE ports.
<a href="#">show power inline</a>	Displays the PoE status for the specified PoE port or for all PoE ports.

**show controllers tcam**

## show controllers tcam

Use the **show controllers tcam** privileged EXEC command to display the state of the registers for all ternary content addressable memory (TCAM) in the system and for all TCAM interface ASICs that are CAM controllers.

**show controllers tcam [asic [number]] [detail]**

<b>Syntax Description</b>	
<b>asic</b>	(Optional) Display port ASIC TCAM information.
<b>number</b>	(Optional) Display information for the specified port ASIC number. The range is from 0 to 15.
<b>detail</b>	(Optional) Display detailed TCAM register information.

**Command Modes** Privileged EXEC

### Command History

**Usage Guidelines** This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

### Examples

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

```
Switch# show controllers tcam
-----
TCAM-0 Registers
-----
REV:    00B30103
SIZE:   00080040
ID:     00000000
CCR:    00000000_F0000020

RPID0:  00000000_00000000
RPID1:  00000000_00000000
RPID2:  00000000_00000000
RPID3:  00000000_00000000

HRR0:   00000000_E000CAF0
HRR1:   00000000_00000000
HRR2:   00000000_00000000
HRR3:   00000000_00000000
HRR4:   00000000_00000000
HRR5:   00000000_00000000
HRR6:   00000000_00000000
HRR7:   00000000_00000000
<output truncated>

GMR31: FF_FFFFFFFF_FFFFFFFF
GMR32: FF_FFFFFFFF_FFFFFFFF
GMR33: FF_FFFFFFFF_FFFFFFFF

=====
TCAM related PortASIC 1 registers
```

```
=====
LookupType:          89A1C67D_24E35F00
LastCamIndex:        0000FFE0
LocalNoMatch:        000069E0
ForwardingRamBaseAddress:
                     00022A00 0002FE00 00040600 0002FE00 0000D400
                     00000000 003FBA00 00009000 00009000 00040600
                     00000000 00012800 00012900
```

Related Commands	Command	Description
	<b>show controllers cpu-interface</b>	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
	<b>show controllers ethernet-controller</b>	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.

---

 show controllers utilization
 

---

# show controllers utilization

Use the **show controllers utilization** command in EXEC mode to display bandwidth utilization on the switch or specific ports.

**show controllers [interface-id] utilization**

<b>Syntax Description</b>	<i>interface-id</i> (Optional) ID of the switch interface.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	
------------------------	--

<b>Examples</b>	This is an example of output from the <b>show controllers utilization</b> command.
-----------------	--

```
Switch# show controllers utilization
Port      Receive Utilization   Transmit Utilization
Fa0/1        0                  0
Fa0/2        0                  0
Fa0/3        0                  0
Fa0/4        0                  0
Fa0/5        0                  0
Fa0/6        0                  0
Fa0/7        0                  0
<output truncated>
<output truncated>

Switch Receive Bandwidth Percentage Utilization : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch# show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

**Table 0-7** *show controllers utilization Field Descriptions*

Field	Description
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Fabric Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

**Related Commands**

Command	Description
<a href="#">show controllers</a>	Displays the interface internal registers.
<a href="#">ethernet-controller</a>	

**show diagnostic**

# show diagnostic

Use the **show diagnostic** command in EXEC mode to view the test results of the online diagnostics and to list the supported test suites.

**show diagnostic content switch [num | all]**

**show diagnostic post**

**show diagnostic result switch [num | all] [detail | test {test-id | test-id-range | all} [detail]]**

**show diagnostic schedule switch [num | all]**

**show diagnostic status**

**show diagnostic switch [num | all] [detail]**

<b>Syntax Description</b>	<b>content</b>	Display test information including test ID, test attributes, and supported coverage test levels for each test and for all modules.
	<b>post</b>	Display the power-on self-test (POST) results; the command output is the same as the <b>show post</b> command.
	<b>result</b>	Displays the test results.
	<b>detail</b>	(Optional) Displays the all test statistics.
	<b>test</b>	Specify a test.
	<i>test-id</i>	Identification number for the test; see the “Usage Guidelines” section for additional information.
	<i>test-id-range</i>	Range of identification numbers for tests; see the “Usage Guidelines” section for additional information.
	<i>all</i>	All the tests.
	<b>schedule</b>	Displays the current scheduled diagnostic tasks.
	<b>status</b>	Displays the test status.

---

**Defaults**

This command has no default settings.

---

**Command Modes**

User EXEC  
Privileged EXEC

---

**Command History**


---

**Usage Guidelines**

If you do not enter a switch *num*, information for all switches is displayed.

In the command output, the possible testing results are as follows:

- Passed (.)
- Failed (F)
- Unknown (U)

**Examples**

This example shows how to display the online diagnostics that are configured on a switch:

```
Switch# show diagnostic content switch 3

Switch 3:
Diagnostics test suite attributes:
  B/* - Basic ondemand test / NA
  P/V/* - Per port test / Per device test / NA
  D/N/* - Disruptive test / Non-disruptive test / NA
  S/* - Only applicable to standby unit / NA
  X/* - Not a health monitoring test / NA
  F/* - Fixed monitoring interval test / NA
  E/* - Always enabled monitoring test / NA
  A/I - Monitoring is active / Monitoring is inactive
  R/* - Switch will reload after test list completion / NA
  P/* - will partition stack / NA

          Test Interval Thre-
ID      Test Name           attributes   day hh:mm:ss.ms shold
===== ====== ====== ====== ====== ====== ====== =====
1)    TestPortAsicStackPortLoopback   B*N****A**  000 00:01:00.00 n/a
2)    TestPortAsicLoopback          B*D*X**IR*  not configured n/a
3)    TestPortAsicCam              B*D*X**IR*  not configured n/a
4)    TestPortAsicRingLoopback     B*D*X**IR*  not configured n/a
5)    TestMicRingLoopback         B*D*X**IR*  not configured n/a
6)    TestPortAsicMem             B*D*X**IR*  not configured n/a
```

This example shows how to display the online diagnostic results for a switch:

```
Switch# show diagnostic result switch 1
Switch 1: SerialNo :
Overall diagnostic result: PASS
Test results: (. = Pass, F = Fail, U = Untested)
1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback -----> .
3) TestPortAsicCam -----> .
4) TestPortAsicRingLoopback -----> .
5) TestMicRingLoopback -----> .
6) TestPortAsicMem -----> .
```

**show diagnostic**

This example shows how to display the online diagnostic test status:

```
Switch# show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
=====
Card      Description          Current Running Test        Run by
-----
1                    N/A
2                    TestPortAsicStackPortLoopback    <OD>
                                         TestPortAsicLoopback      <OD>
                                         TestPortAsicCam        <OD>
                                         TestPortAsicRingLoopback <OD>
                                         TestMicRingLoopback     <OD>
                                         TestPortAsicMem        <OD>
3                    N/A
4                    N/A
=====
Switch#
```

This example shows how to display the online diagnostic test schedule for a switch:

```
Switch# show diagnostic schedule switch 1
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">clear ip arp inspection statistics</a>	Configures the health-monitoring diagnostic test.
<a href="#">diagnostic schedule</a>	Sets the scheduling of test-based online diagnostic testing.
<a href="#">diagnostic start</a>	Starts the online diagnostic test.

# show dot1x

Use the **show dot1x** command in EXEC mode to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

**show dot1x [{all [summary] | interface *interface-id*} [details | statistics]]**

## Syntax Description

<b>all [summary]</b>	(Optional) Display the IEEE 802.1x status for all ports.
<b>interface <i>interface-id</i></b>	<b>Note</b> (Optional) Display the IEEE 802.1x status for the specified port (including type, module, and port number)
<b>details</b>	(Optional) Display the IEEE 802.1x interface details.
<b>statistics</b>	(Optional) Display IEEE 802.1x statistics for the specified port.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.2(25)SED	The display was expanded to include <b>auth-fail-vlan</b> in the authorization state machine state and port status fields.
12.2(25)SEE	The command syntax was changed, and the command output was modified.

## Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

If the port control is configured as unidirectional or bidirectional control and this setting conflicts with the switch configuration, the **show dot1x {all | interface *interface-id*}** privileged EXEC command output has this information:

ControlDirection = In (Inactive)

## Examples

This is an example of output from the **show dot1x** command:

```
Switch# show dot1x
Sysauthcontrol          Enabled
Dot1x Protocol Version   2
Critical Recovery Delay  100
Critical EAPOL          Disabled
```

This is an example of output from the **show dot1x all** command:

```
Switch# show dot1x all
Sysauthcontrol          Enabled
Dot1x Protocol Version   2
Critical Recovery Delay  100
Critical EAPOL          Disabled

Dot1x Info for GigabitEthernet0/1
```

■ show dot1x

```

PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
Violation Mode = PROTECT
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

<output truncated>

```

This is an example of output from the **show dot1x all summary** command:

Interface	PAE	Client	Status
Gi0/1	AUTH	none	UNAUTHORIZED
Gi0/2	AUTH	00a0.c9b8.0072	AUTHORIZED
Gi0/3	AUTH	none	UNAUTHORIZED

This is an example of output from the **show dot1x interface *interface-id*** command:

```

Switch# show dot1x interface gigabitethernet0/2
Dot1x Info for GigabitEthernet0/2
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = In
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

```

This is an example of output from the **show dot1x interface *interface-id* details** command:

```

Switch# show dot1x interface gigabitethernet0/2 details
Dot1x Info for GigabitEthernet0/2
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

```

Dot1x Authenticator Client List Empty

This is an example of output from the **show dot1x interface *interface-id* details** command when a port is assigned to a guest VLAN and the host mode changes to multiple-hosts mode:

```
Switch# show dot1x interface gigabitethernet0/1 details
Dot1x Info for GigabitEthernet0/1
-----
PAE          = AUTHENTICATOR
PortControl   = AUTO
ControlDirection = Both
HostMode      = SINGLE_HOST
ReAuthentication = Enabled
QuietPeriod    = 60
ServerTimeout  = 30
SuppTimeout    = 30
ReAuthPeriod   = 3600 (Locally configured)
ReAuthMax      = 2
MaxReq         = 2
TxPeriod       = 30
RateLimitPeriod = 0
Guest-Vlan     = 182

Dot1x Authenticator Client List Empty

Port Status      = AUTHORIZED
Authorized By    = Guest-Vlan
Operational HostMode = MULTI_HOST
Vlan Policy      = 182
```

This is an example of output from the **show dot1x interface *interface-id* statistics** command. [Table 2-32](#) describes the fields in the display.

```
Switch# show dot1x interface gigabitethernet0/2 statistics
Dot1x Authenticator Port Statistics for GigabitEthernet0/2
-----
RxStart = 0      RxLogoff = 0      RxResp = 1      RxRespID = 1
RxInvalid = 0    RxLenErr = 0     RxTotal = 2

TxReq = 2        TxReqID = 132    TxTotal = 134

RxVersion = 2    LastRxSrcMAC = 00a0.c9b8.0072
```

**Table 0-8** *show dot1x statistics Field Descriptions*

Field	Description
RxStart	Number of valid EAPOL-start frames that have been received.
RxLogoff	Number of EAPOL-logoff frames that have been received.
RxResp	Number of valid EAP-response frames (other than response/identity frames) that have been received.
RxRespID	Number of EAP-response/identity frames that have been received.
RxInvalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
RxLenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
RxTotal	Number of valid EAPOL frames of any type that have been received.

show dot1x

**Table 0-8** show dot1x statistics Field Descriptions (continued)

Field	Description
TxReq	Number of EAP-request frames (other than request/identity frames) that have been sent.
TxReqId	Number of Extensible Authentication Protocol (EAP)-request/identity frames that have been sent.
TxTotal	Number of Extensible Authentication Protocol over LAN (EAPOL) frames of any type that have been sent.
RxVersion	Number of received packets in the IEEE 802.1x Version 1 format.
LastRxSrcMac	Source MAC address carried in the most recently received EAPOL frame.

**Related Commands**

Command	Description
<a href="#">dot1x default</a>	Resets the IEEE 802.1x parameters to their default values.

# show dtp

Use the **show dtp** privileged EXEC command to display Dynamic Trunking Protocol (DTP) information for the switch or for a specified interface.

**show dtp [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface</b> (Optional) Display port security settings for the specified interface. Valid interfaces <i>interface-id</i> include physical ports (including type, module, and port number).
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

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

```
Switch# show dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    21 interfaces using DTP
```

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

```
Switch# show dtp interface gigabitethernet0/1
DTP information for GigabitEthernet0/1:
    TOS/TAS/TNS:                                ACCESS/AUTO/ACCESS
    TOT/TAT/TNT:                                NATIVE/NEGOTIATE/NATIVE
    Neighbor address 1:                          000943A7D081
    Neighbor address 2:                          000000000000
    Hello timer expiration (sec/state):        1/RUNNING
    Access timer expiration (sec/state):       never/STOPPED
    Negotiation timer expiration (sec/state): never/STOPPED
    Multidrop timer expiration (sec/state):   never/STOPPED
    FSM state:                                 S2:ACCESS
    # times multi & trunk:                   0
    Enabled:                                    yes
    In STP:                                     no

    Statistics
    -----
    3160 packets received (3160 good)
    0 packets dropped
        0 nonegotiate, 0 bad version, 0 domain mismatches, 0 bad TLVs, 0 other
    6320 packets output (6320 good)
        3160 native
        0 output errors
        0 trunk timeouts
        1 link ups, last link up on Mon Mar 01 1993, 01:02:29
        0 link downs
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show interfaces trunk</a>	Displays interface trunking information.

**show eap**

## show eap

Use the **show eap** privileged EXEC command to display Extensible Authentication Protocol (EAP) registration and session information for the switch or for the specified port.

```
show eap { {registrations [method [name] | transport [name]]} | {sessions [credentials name [interface interface-id] | interface interface-id | method name | transport name]} } [credentials name | interface interface-id | transport name]
```

### Syntax Description

<b>registrations</b>	Display EAP registration information.
<b>method name</b>	(Optional) Display EAP method registration information.
<b>transport name</b>	(Optional) Display EAP transport registration information.
<b>sessions</b>	Display EAP session information.
<b>credentials name</b>	(Optional) Display EAP method registration information.
<b>interface interface-id</b>	<b>Note</b> (Optional) Display the EAP information for the specified port (including type, module, and port number).

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(25)SEE	This command was introduced.

### Usage Guidelines

When you use the **show eap registrations** privileged EXEC command with these keywords, the command output shows this information:

- None—All the lower levels used by EAP and the registered EAP methods.
- **method name** keyword—The specified method registrations.
- **transport name** keyword—The specific lower-level registrations.

When you use the **show eap sessions** privileged EXEC command with these keywords, the command output shows this information:

- None—All active EAP sessions.
- **credentials name** keyword—The specified credentials profile.
- **interface interface-id** keyword—The parameters for the specified interface.
- **method name** keyword—The specified EAP method.
- **transport name** keyword—The specified lower layer.

**Examples**

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

```
Switch# show eap registrations
Registered EAP Methods:
  Method  Type          Name
    4      Peer          MD5

Registered EAP Lower Layers:
  Handle  Type          Name
    2      Authenticator Dot1x-Authenticator
    1      Authenticator MAB
```

This is an example of output from the **show eap registrations transport all** command:

```
Switch# show eap registrations transport all
Registered EAP Lower Layers:
  Handle  Type          Name
    2      Authenticator Dot1x-Authenticator
    1      Authenticator MAB
```

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

```
Switch# show eap sessions
Role:           Authenticator  Decision:          Fail
Lower layer:    Dot1x-AuthenticaInterface:        Gi0/1
Current method: None                      Method state:  Uninitialised
Retransmission count: 0 (max: 2)   Timer:          Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle:     0x5200000A    Credentials profile: None
Lower layer context ID: 0x93000004  Eap profile name: None
Method context ID: 0x00000000  Peer Identity:    None
Start timeout (s): 1                  Retransmit timeout (s): 30 (30)
Current ID:      2                  Available local methods: None

Role:           Authenticator  Decision:          Fail
Lower layer:    Dot1x-AuthenticaInterface:        Gi0/2
Current method: None                      Method state:  Uninitialised
Retransmission count: 0 (max: 2)   Timer:          Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle:     0xA800000B    Credentials profile: None
Lower layer context ID: 0x0D000005  Eap profile name: None
Method context ID: 0x00000000  Peer Identity:    None
Start timeout (s): 1                  Retransmit timeout (s): 30 (30)
Current ID:      2                  Available local methods: None

<Output truncated>
```

This is an example of output from the **show eap sessions interface *interface-id*** privileged EXEC command:

```
Switch# show eap sessions gigabitethernet0/1
Role:           Authenticator  Decision:          Fail
Lower layer:    Dot1x-AuthenticaInterface:        Gi0/1
Current method: None                      Method state:  Uninitialised
Retransmission count: 1 (max: 2)   Timer:          Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle:     0x5200000A    Credentials profile: None
Lower layer context ID: 0x93000004  Eap profile name: None
Method context ID: 0x00000000  Peer Identity:    None
Start timeout (s): 1                  Retransmit timeout (s): 30 (30)
Current ID:      2                  Available local methods: None
```

■ show eap

Related Commands	Command	Description
	<a href="#">clear eap sessions</a>	Clears EAP session information for the switch or for the specified port.

# show env

Syntax Description	
<b>all</b>	Display both fan and temperature environmental status.
<b>fan</b>	Display the switch fan status.
<b>power</b>	Display the switch power status.
<b>temperature</b>	Display the switch temperature status.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

## Usage Guidelines

## Examples

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

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

```
Switch# show env fan
FAN is OK
```

---

 show errdisable detect
 

---

# show errdisable detect

Use the **show errdisable detect** command in EXEC mode to display error-disabled detection status.

**show errdisable detect**

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Usage Guidelines** A displayed `gbic-invalid` error reason refers to an invalid small form-factor pluggable (SFP) module.

## Examples

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

```
Switch# show errdisable detect
ErrDisable Reason      Detection      Mode
-----  -----  -----
arp-inspection          Enabled       port
bpduguard               Enabled       vlan
channel-misconfig        Enabled       port
community-limit          Enabled       port
dhcp-rate-limit          Enabled       port
dtp-flap                Enabled       port
gbic-invalid             Enabled       port
inline-power              Enabled       port
invalid-policy            Enabled       port
link-flap                Enabled       port
loopback                 Enabled       port
lsgroup                  Enabled       port
pagp-flap                Enabled       port
psecure-violation         Enabled       port/vlan
security-violatio         Enabled       port
sfp-config-mismat        Enabled       port
storm-control             Enabled       port
udld                     Enabled       port
vmps                     Enabled       port
```

## Related Commands

Command	Description
<a href="#">errdisable detect cause</a>	Enables error-disabled detection for a specific cause or all causes.
<a href="#">show errdisable flap-values</a>	Displays error condition recognition information.
<a href="#">show errdisable recovery</a>	Displays error-disabled recovery timer information.
<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in error-disabled state.

# show errdisable flap-values

Use the **show errdisable flap-values** command in EXEC mode to display conditions that cause an error to be recognized for a cause.

## show errdisable flap-values

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Usage Guidelines** The *Flaps* column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. For example, the display shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval.

ErrDisable Reason	Flaps	Time (sec)
pagp-flap	3	30
dtp-flap	3	30
link-flap	5	10

## Examples

This is an example of output from the **show errdisable flap-values** command:

```
Switch# show errdisable flap-values
-----
```

ErrDisable Reason	Flaps	Time (sec)
pagp-flap	3	30
dtp-flap	3	30
link-flap	5	10

## Related Commands

Command	Description
<a href="#">errdisable detect cause</a>	Enables error-disabled detection for a specific cause or all causes.
<a href="#">show errdisable detect</a>	Displays error-disabled detection status.
<a href="#">show errdisable recovery</a>	Displays error-disabled recovery timer information.
<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in error-disabled state.

■ show errdisable recovery

# show errdisable recovery

Use the **show errdisable recovery** command in EXEC mode to display the error-disabled recovery timer information.

**show errdisable recovery**

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Usage Guidelines** A *gbic-invalid error-disable* reason refers to an invalid small form-factor pluggable (SFP) module interface.

**Examples** This is an example of output from the **show errdisable recovery** command:

```
Switch# show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                  Disabled
bpduguard             Disabled
security-violatio     Disabled
channel-misconfig     Disabled
vmps                 Disabled
pagp-flap              Disabled
dtp-flap              Disabled
link-flap              Enabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood          Disabled
storm-control          Disabled
arp-inspection         Disabled
loopback               Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:

Interface    Errdisable reason      Time left(sec)
-----
Gi0/2        link-flap            279
```



**Note**

Though visible in the output, the unicast-flood field is not valid.

## Related Commands

Command	Description
<a href="#">errdisable recovery</a>	Configures the recover mechanism variables.
<a href="#">show errdisable detect</a>	Displays error-disabled detection status.
<a href="#">show errdisable flap-values</a>	Displays error condition recognition information.
<a href="#">show interfaces status</a>	Displays interface status or a list of interfaces in error-disabled state.

---

 show etherchannel
 

---

# show etherchannel

Use the **show etherchannel** command in EXEC mode to display EtherChannel information for a channel.

```
show etherchannel [channel-group-number {detail | port | port-channel | protocol | summary}]
{detail | load-balance | port | port-channel | protocol | summary}
```

---

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to .
<b>detail</b>	Display detailed EtherChannel information.
<b>load-balance</b>	Display the load-balance or frame-distribution scheme among ports in the port channel.
<b>port</b>	Display EtherChannel port information.
<b>port-channel</b>	Display port-channel information.
<b>protocol</b>	Display the protocol that is being used in the EtherChannel.
<b>summary</b>	Display a one-line summary per channel-group.

---



---

## Command Modes

User EXEC  
Privileged EXEC

---

## Command History

---

## Usage Guidelines

If you do not specify a *channel-group*, all channel groups are displayed.

---

## Examples

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch# show etherchannel 1 detail
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
          Ports in the group:
          -----
Port: Gi0/1
          -----
Port state      = Up Mstr In-Bndl
Channel group  = 1           Mode = Active      Gcchange = -
Port-channel   = Po1         GC   = -           Pseudo port-channel = Po1
Port index     = 0           Load = 0x00       Protocol = LACP
Flags: S - Device is sending Slow LACPDU   F - Device is sending fast LACPDU
          A - Device is in active mode.        P - Device is in passive mode.
Local information:
          LACP port      Admin      Oper      Port      Port
Port    Flags    State    Priority    Key      Key      Number    State
          -----
Age of the port in the current state: 01d:20h:06m:04s
```

```

Port-channels in the group:
-----
Port-channel: Po1      (Primary Aggregator)
-----
Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1           Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            = LACP

```

Ports in the Port-channel:

Index	Load	Port	EC state	No of bits
-------	------	------	----------	------------

```
Time since last port bundled:    01d:20h:20m:20s    Gi0/2
```

This is an example of output from the **show etherchannel 1 summary** command:

```

Switch# show etherchannel 1 summary
Flags: D - down      P - in port-channel
       I - stand-alone S - suspended
       H - Hot-standby (LACP only)
       R - Layer3      S - Layer2
       u - unsuitable for bundling
       U - in use       f - failed to allocate aggregator
       d - default port

```

```
Number of channel-groups in use: 1
```

```
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

**show etherchannel**

This is an example of output from the **show etherchannel 1 port-channel** command:

```
Switch# show etherchannel 1 port-channel
      Port-channels in the group:
      -----
      Port-channel: Po1      (Primary Aggregator)
      -----
      Age of the Port-channel = 01d:20h:24m:50s
      Logical slot/port = 10/1           Number of ports = 2
      HotStandBy port = null
      Port state          = Port-channel Ag-Inuse
      Protocol            = LACP

      Ports in the Port-channel:
      Index   Load   Port       EC state        No of bits
      -----+-----+-----+-----+
      Time since last port bundled: 01d:20h:24m:44s    Gi0/2
```

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

```
Switch# show etherchannel protocol
      Channel-group listing:
      -----
      Group: 1
      -----
      Protocol: LACP

      Group: 2
      -----
      Protocol: PAgP
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>channel-group</b></a>	Assigns an Ethernet port to an EtherChannel group.
<a href="#"><b>channel-protocol</b></a>	Restricts the protocol used on a port to manage channeling.
<a href="#"><b>interface port-channel</b></a>	Accesses or creates the port channel.

# show fallback profile

Use the **show fallback profile** privileged EXEC command to display the fallback profiles that are configured on a switch.

## show fallback profile

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

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** Use the **show fallback profile** privileged EXEC command to display profiles that are configured on the switch.

## Examples

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

```
switch# show fallback profile
Profile Name: dot1x-www
-----
Description      : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----
Description      : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----
Description      : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

## Related Commands

	<b>Command</b>	<b>Description</b>
	<a href="#"><b>dot1x fallback profile</b></a>	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	<a href="#"><b>fallback profile profile</b></a>	Create a web authentication fallback profile.
	<a href="#"><b>ip admission rule</b></a>	Enable web authentication on a switch port
	<a href="#"><b>ip admission name proxy http</b></a>	Enable web authentication globally on a switch
	<a href="#"><b>show dot1x [interface interface-id]</b></a>	Displays IEEE 802.1x status for the specified port.

**show flowcontrol**

# show flowcontrol

Use the **show flowcontrol** command in EXEC mode to display the flow control status and statistics.

**show flowcontrol [interface *interface-id* | module *number*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Display the flow control status and statistics for a specific interface. <b>module <i>number</i></b> (Optional) Display the flow control status and statistics for all interfaces on the . This option is not available if you have entered a specific interface ID.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Usage Guidelines

Use this command to display the flow control status and statistics on the switch or for a specific interface.

Use the **show flowcontrol** command to display information about all the switch interfaces. he output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module number** command.

Use the **show flowcontrol interface *interface-id*** command to display information about a specific interface.

## Examples

This is an example of output from the **show flowcontrol** command.

```
Switch# show flowcontrol
Port      Send FlowControl  Receive FlowControl RxPause TxPause
          admin     oper      admin     oper
----- -----
Gi0/1    Unsupp.   Unsupp.   off      off      0      0
Gi0/2    desired   off      off      off      0      0
Gi0/3    desired   off      off      off      0      0
<output truncated>
```

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

```
Switch# show flowcontrol gigabitethernet0/2
Port      Send FlowControl  Receive FlowControl RxPause TxPause
          admin     oper      admin     oper
----- -----
```

## Related Commands

<b>Command</b>	<b>Description</b>
<a href="#"><b>flowcontrol</b></a>	Sets the receive flow-control state for an interface.

# show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

```
show interfaces [interface-id | vlan vlan-id] [accounting | capabilities [module number] |
  counters | description | etherchannel | flowcontrol | pruning | stats | status [err-disabled] |
  switchport [backup | module number] | transceiver | properties | detail [module number] |
  trunk]
```

Syntax Description	<b>interface-id</b>	(Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to .
	<b>vlan vlan-id</b>	(Optional) VLAN identification. The range is 1 to 4094.
	<b>accounting</b>	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets.  <b>Note</b> The display shows only packets processed in software; hardware-switched packets do not appear.
	<b>capabilities</b>	(Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
	<b>module number</b>	<b>Note</b> (Optional) Display <b>capabilities</b> , <b>switchport</b> configuration, or <b>transceiver</b> characteristics (depending on preceding keyword) of all interfaces on the . This option is not available if you enter a specific interface ID.
	<b>counters</b>	(Optional) See the <b>show interfaces counters</b> command.
	<b>description</b>	(Optional) Display the administrative status and description set for an interface.
	<b>etherchannel</b>	(Optional) Display interface EtherChannel information.
	<b>flowcontrol</b>	(Optional) Display interface flowcontrol information
	<b>pruning</b>	(Optional) Display interface trunk VTP pruning information.
	<b>stats</b>	(Optional) Display the input and output packets by switching path for the interface.
	<b>status</b>	(Optional) Display the status of the interface. A status of <i>unsupported</i> in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
	<b>err-disabled</b>	(Optional) Display interfaces in error-disabled state.
	<b>switchport</b>	(Optional) Display the administrative and operational status of a switching port, including port blocking and port protection settings.
	<b>backup</b>	(Optional) Display Flex Link backup interface configuration and status for the specified interface or all interfaces on the .

**show interfaces**


---

<b>transceiver [detail   properties]</b>	(Optional) Display the physical properties of a CWDM or DWDM small form-factor (SFP) module interface. The keywords have these meanings:
	<ul style="list-style-type: none"> <li>• <b>detail</b>—(Optional) Display calibration properties, including high and low numbers and any alarm information.</li> <li>• <b>properties</b>—(Optional) Display .</li> </ul>
<b>trunk</b>	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

---



---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

---

**Command History****Usage Guidelines**

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interfaces interface-id capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces .



Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

---

**Examples**

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

```
Switch# show interfaces gigabitethernet
GigabitEthernet0 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
  Last clearing of "show interfaces" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2 packets input, 1040 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    4 packets output, 1040 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces accounting** command.

```

Switch# show interfaces accounting
Vlan1
      Protocol   Pkts In   Chars In   Pkts Out   Chars Out
          IP       1094395  131900022  559555    84077157
          Spanning Tree  283896   17033760      42      2520
          ARP        63738    3825680     231     13860
Interface Vlan2 is disabled
Vlan7
      Protocol   Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
Vlan31
      Protocol   Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

GigabitEthernet0/1
      Protocol   Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
      Protocol   Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<output truncated>

```

This is an example of output from the **show interfaces capabilities** command for an interface.

```

Switch# show interfaces gigabitethernet0/2 capabilities
GigabitEthernet0/2
Type:           10/100/1000BaseTX
Speed:          10,100,1000,auto
Duplex:         full,auto
Trunk encaps. type: 802.1Q, ISL
Trunk mode:      on,off,desirable,nonegotiate
Channel:        yes
Broadcast suppression: percentage(0-100)
Flowcontrol:    rx-(off,on,desired),tx-(none)
Fast Start:     yes
QoS scheduling: rx-(not configurable on per port basis),tx-(4q2t)
CoS rewrite:    yes
ToS rewrite:    yes
UDLD:           yes
Inline power:   no
SPAN:            source/destination
PortSecure:     yes
Dot1x:           yes
Multiple Media Types: rj45, sfp, auto-select

```

This is an example of output from the **show interfaces interface description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```

Switch# show interfaces gigabitethernet0/2 description
Interface Status      Protocol Description

```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```

Switch# show interfaces etherchannel
-----
Port-channel1:
Age of the Port-channel = 03d:20h:17m:29s
Logical slot/port = 10/1           Number of ports = 0
GC                = 0x00000000       HotStandBy port = null
Port state        = Port-channel Ag-Not-Inuse

```

**show interfaces**

```

Port-channel2:
Age of the Port-channel = 03d:20h:17m:29s
Logical slot/port = 10/2 Number of ports = 0
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel = 03d:20h:17m:29s
Logical slot/port = 10/3 Number of ports = 0
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse

```

This is an example of output from the **show interfaces interface-id pruning** command when pruning is enabled in the VTP domain:

```

Switch# show interfaces gigabitethernet0/2 pruning
Port    Vlans pruned for lack of request by neighbor

Port    Vlans traffic requested of neighbor

```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface.

```

Switch# show interfaces vlan 1 stats
Switching path   Pkts In   Chars In   Pkts Out   Chars Out
      Processor   1165354   136205310   570800   91731594
      Route cache     0         0         0         0
      Total       1165354   136205310   570800   91731594

```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces.

```
Switch# show interfaces status
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state.

```
Switch# show interfaces status err-disabled
Port      Name          Status        Reason
```

This is an example of output from the **show interfaces switchport** command for a port. [Table 2-34](#) describes the fields in the display.

**Note**

Private VLAN are not supported, so those fields are not applicable.

```

Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association:10 (VLAN0010) 502 (VLAN0502)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none

```

```

Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none

```

**Table 0-9** *show interfaces switchport Field Descriptions*

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode	Displays the administrative and operational modes.
Operational Mode	
Administrative Trunking Encapsulation	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Operational Trunking Encapsulation	
Negotiation of Trunking	
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Trunking VLANs Enabled	
Trunking VLANs Active	
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Unknown multicast blocked	
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

<sup>1</sup>This is an example of output from the **show interfaces switchport backup** command:

```

Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
      Active Interface    Backup Interface    State
      -----
      Fa0/1                Fa0/2            Active Up/Backup Standby
      Fa0/3                Fa0/5            Active Down/Backup Up
      Po1                  Po2             Active Standby/Backup Up

```

This is an example of output from the **show interfaces switchport backup** command. In this example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)#interface gigabitEthernet 0/6
```

**show interfaces**

```
Switch(config-if)#switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gi0/8 forwards traffic for VLANs 60, 100 to 120, and Gi0/6 forwards traffic for VLANs 1 to 50.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

Vlans on Interface Gi 0/6: 1-50  
Vlans on Interface Gi 0/8: 60, 100-120

When a Flex Link interface goes down (LINK\_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

Vlans on Interface Gi 0/6:  
Vlans on Interface Gi 0/8: 1-50, 60, 100-120

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi0/6 comes up, then VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

Vlans on Interface Gi 0/6: 1-50  
Vlans on Interface Gi 0/8: 60, 100-120

This is an example of output from the **show interfaces interface-id pruning** command:

```
Switch# show interfaces gigabitethernetpruning
Port      Vlans pruned for lack of request by neighbor
```

This is an example of output from the **show interfaces interface-id trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernettrunk
Port      Mode      Encapsulation  Status      Native vlan
Gi0/1    auto      negotiate     trunking      1

Port      Vlans allowed on trunk
Gi0/1    1-4094

Port      Vlans allowed and active in management domain
Gi0/1    1-4

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1    1-4
```

This is an example of output from the **show interfaces interface-id transceiver properties** command:

```
Switch# show interfaces gigabitethernettransceiver properties
Name : Gi0/2
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Operational Duplex: auto
Administrative Auto-MDIx: off
Operational Auto-MDIx: off
```

This is an example of output from the **show interfaces interface-id transceiver detail** command:

```
Switch# show interfaces gigabitethernettransceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

		High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Port	Temperature (Celsius)	(Celsius)	(Celsius)	(Celsius)	(Celsius)
Gi0/3	41.5	110.0	103.0	-8.0	-12.0
		High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Port	Voltage (Volts)	(Volts)	(Volts)	(Volts)	(Volts)
Gi0/3	3.20	4.00	3.70	3.00	2.95
		High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Port	Current (milliamperes)	(mA)	(mA)	(mA)	(mA)
Gi0/3	31.0	84.0	70.0	4.0	2.0
		High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Port	Optical Transmit Power (dBm)	(dBm)	(dBm)	(dBm)	(dBm)
Gi0/3	-0.0 ( -0.0 )	-0.0	-0.0	-0.0	-0.0
		High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Port	Optical Receive Power (dBm)	(dBm)	(dBm)	(dBm)	(dBm)
Gi0/3	N/A ( -0.0 ) --	-0.0	-0.0	-0.0	-0.0

### Related Commands

Command	Description
<a href="#">switchport access</a>	Configures a port as a static-access or a dynamic-access port.
<a href="#">switchport block</a>	Blocks unknown unicast or multicast traffic on an interface.
<a href="#">switchport backup interface</a>	Configures Flex Links, a pair of Layer 2 interfaces that provide mutual backup.
<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.

**show interfaces**

Command	Description
<b>switchport protected</b>	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.
<b>switchport trunk pruning</b>	Configures the VLAN pruning-eligible list for ports in trunking mode.

# show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for the switch or for a specific interface.

**show interfaces [interface-id | vlan *vlan-id*] counters [errors | etherchannel | protocol status | trunk]**

<b>Syntax Description</b>	
<b>interface-id</b>	(Optional) ID of the physical interface.
<b>errors</b>	(Optional) Display error counters.
<b>etherchannel</b>	(Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
<b>protocol status</b>	(Optional) Display status of protocols enabled on interfaces.
<b>trunk</b>	(Optional) Display trunk counters.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** If you do not enter any keywords, all counters for all interfaces are included.



**Note** Though visible in the command-line help string, the **vlan *vlan-id*** keyword is not supported.

## Examples

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port          InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi0/1           0            0            0            0
Gi0/2           0            0            0            0
<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces.

```
Switch# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
```

**show interfaces counters**

```
Vlan3500: Other, IP
FastEthernet0/1: Other, IP, ARP, CDP
FastEthernet0/2: Other, IP
FastEthernet0/3: Other, IP
FastEthernet0/4: Other, IP
FastEthernet0/5: Other, IP
FastEthernet0/6: Other, IP
FastEthernet0/7: Other, IP
FastEthernet0/8: Other, IP
FastEthernet0/9: Other, IP
FastEthernet0/10: Other, IP, CDP

<output truncated>
```

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Switch# show interfaces counters trunk
Port      TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1          0            0            0
Gi0/2          0            0            0
Gi0/3        80678         4155           0
Gi0/4        82320         126            0
Gi0/5          0            0            0

<output truncated>
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show interfaces</b></a>	Displays additional interface characteristics.

# show interfaces transceivers

Use the **show interfaces transceivers** privileged EXEC command to display the physical properties of a small form-factor pluggable (SFP) module interface.

**show interfaces [interface-id] transceiver [detail | dom-supported-list | module number | properties | threshold-table]**



**Note** This command is supported only in Catalyst 2960-S switches.

<b>Syntax Description</b>	
<b>interface-id</b>	(Optional) Display configuration and status for a specified physical interface.
<b>detail</b>	(Optional) Display calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
<b>dom-supported-list</b>	(Optional) List all supported DoM transceivers.
<b>module number</b>	(Optional) Limit display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
<b>properties</b>	(Optional) Display speed, duplex, and inline power settings on an interface.
<b>threshold-table</b>	(Optional) Display alarm and warning threshold table

<b>Command Modes</b>	User EXEC
----------------------	-----------

## Command History

### Examples

This is an example of output from the **show interfaces interface-id transceiver properties** command:

```
Switch# show interfaces gigabitethernet1/0/1 transceiver properties
Name : Gi1/0/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

This is an example of output from the **show interfaces interface-id transceiver detail** command:

```
Switch# show interfaces gigabitethernet1/0/3 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is externally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

	High Alarm	High Warn	Low Warn	Low Alarm
Temperature	Threshold	Threshold	Threshold	Threshold

**show interfaces transceivers**

Port	(Celsius)	(Celsius)	(Celsius)	(Celsius)	(Celsius)
Gi1/0/3	41.5	110.0	103.0	-8.0	-12.0
	Voltage Port (Volts)		High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)
Gi1/0/3	3.20	4.00	3.70	3.00	2.95
	Current Port (milliamperes)		High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)
Gi1/0/3	31.0	84.0	70.0	4.0	2.0
	Optical Transmit Power Port (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)
Gi1/0/3	-0.0 (-0.0)	-0.0	-0.0	-0.0	-0.0
	Optical Receive Power Port (dBm)		High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)
Gi1/0/3	N/A (-0.0) --	-0.0	-0.0	-0.0	-0.0

This is an example of output from the **show interfaces transceiver dom-supported-list** command:

```
Switch# show interfaces transceiver dom-supported-list
Transceiver Type          Cisco p/n min version
                           supporting DOM
-----
DWDM GBIC                ALL
DWDM SFP                 ALL
RX only WDM GBIC         ALL
DWDM XENPAK               ALL
DWDM X2                   ALL
DWDM XFP                 ALL
CWDM GBIC                NONE
CWDM X2                   ALL
CWDM XFP                 ALL
XENPAK ZR                ALL
X2 ZR                    ALL
XFP ZR                   ALL
Rx_only_WDM_XENPAK        ALL
XENPAK_ER                10-1888-03
X2_ER                    ALL
XFP_ER                   ALL
XENPAK_LR                10-1838-04
X2_LR                     ALL
<output truncated>
```

This is an example of output from the **show interfaces transceiver threshold-table** command:

Optical Tx	Optical Rx	Temp	Laser Bias	Voltage current	
DWDM GBIC					
Min1	-0.50	-28.50	0	N/A	4.50
Min2	-0.30	-28.29	5	N/A	4.75

Max2	3.29	-6.69	60	N/A	5.25
Max1	3.50	6.00	70	N/A	5.50
DWDM SFP					
Min1	-0.50	-28.50	0	N/A	3.00
Min2	-0.30	-28.29	5	N/A	3.09
Max2	4.30	-9.50	60	N/A	3.59
Max1	4.50	9.30	70	N/A	3.70
RX only WDM GBIC					
Min1	N/A	-28.50	0	N/A	4.50
Min2	N/A	-28.29	5	N/A	4.75
Max2	N/A	-6.69	60	N/A	5.25
Max1	N/A	6.00	70	N/A	5.50
DWDM XENPAK					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM X2					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
DWDM XFP					
Min1	-1.50	-24.50	0	N/A	N/A
Min2	-1.29	-24.29	5	N/A	N/A
Max2	3.29	-6.69	60	N/A	N/A
Max1	3.50	4.00	70	N/A	N/A
CWDM X2					
Min1	N/A	N/A	0	N/A	N/A
Min2	N/A	N/A	0	N/A	N/A
Max2	N/A	N/A	0	N/A	N/A
Max1	N/A	N/A	0	N/A	N/A

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show interfaces</a>	Displays additional interface characteristics.

**show inventory**

# show inventory

Use the **show inventory** command in EXEC mode to display product identification (PID) information for the hardware.

**show inventory [entity-name | raw]**

<b>Syntax Description</b>	<table border="0"> <tr> <td><i>entity-name</i></td><td>(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet0/1) into which a small form-factor pluggable (SFP) module is installed.</td></tr> <tr> <td><b>raw</b></td><td>(Optional) Display every entity in the device.</td></tr> </table>	<i>entity-name</i>	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet0/1) into which a small form-factor pluggable (SFP) module is installed.	<b>raw</b>	(Optional) Display every entity in the device.
<i>entity-name</i>	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet0/1) into which a small form-factor pluggable (SFP) module is installed.				
<b>raw</b>	(Optional) Display every entity in the device.				

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Usage Guidelines

The command is case sensitive. With no arguments, the **show inventory** command produces a compact dump of all identifiable entities that have a product identifier. The compact dump displays the entity location (slot identity), entity description, and the unique device identifier (UDI) (PID, VID, and SN) of that entity.


**Note**

If there is no PID, no output appears when you enter the **show inventory** command.

---

### Examples

This is example output from the **show inventory** command:

# show ip arp inspection

Use the **show ip arp inspection** privileged EXEC command to display the configuration and the operating state of dynamic Address Resolution Protocol (ARP) inspection or the status of this feature for all VLANs or for the specified interface or VLAN.

```
show ip arp inspection [interfaces [interface-id] | log | statistics [vlan vlan-range] | vlan
vlan-range]
```

<b>Syntax Description</b>	<b>interfaces</b> [ <i>interface-id</i> ] <b>log</b> <b>statistics</b> [ <b>vlan</b> <i>vlan-range</i> ] <b>vlan</b> <i>vlan-range</i>	(Optional) Display the trust state and the rate limit of ARP packets for the specified interface or all interfaces. Valid interfaces include physical ports and port channels. (Optional) Display the configuration and contents of the dynamic ARP inspection log buffer. (Optional) Display statistics for forwarded, dropped, MAC validation failure, IP validation failure, access control list (ACL) permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, display information only for VLANs with dynamic ARP inspection enabled (active). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. (Optional) Display the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, display information only for VLANs with dynamic ARP inspection enabled (active). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
---------------------------	---	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

**Examples** This is an example of output from the **show ip arp inspection** command

```
Switch# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation     : Enabled

Vlan      Configuration    Operation   ACL Match      Static ACL
----      -----          -----      -----          -----
      1       Enabled        Active      deny-all      No

Vlan      ACL Logging     DHCP Logging  Probe Logging
----      -----          -----          -----
```

**show ip arp inspection**

		Acl-Match	All	Permit	
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops	
1	0	0	0	0	
Vlan	DHCP Permits	ACL Permits	Probe Permits	Source MAC Failures	
1	0	0	0	0	
Vlan	Dest MAC Failures	IP Validation Failures	Invalid Protocol Data		
1	0	0	0	0	

This is an example of output from the **show ip arp inspection interfaces** command:

```
Switch# show ip arp inspection interfaces
Interface      Trust State     Rate (pps)    Burst Interval
-----          -----          -----          -----
Gi0/1          Untrusted      15              1
Gi0/2          Untrusted      15              1
Gi0/3          Untrusted      15              1
```

This is an example of output from the **show ip arp inspection interfaces interface-id** command:

```
Switch# show ip arp inspection interfaces gigabitethernet
Interface      Trust State     Rate (pps)    Burst Interval
-----          -----          -----          -----
Gi0/1          Untrusted      15              1
```

This is an example of output from the **show ip arp inspection log** command. It shows the contents of the log buffer before the buffers are cleared:

```
Switch# show ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 10 entries per 300 seconds.

Interface  Vlan  Sender MAC        Sender IP      Num Pkts  Reason      Time
-----      ---   -----          -----          -----      -----      -----
Gi0/1      5     0003.0000.d673  192.2.10.4      5  DHCP Deny   19:39:01 UTC
Mon Mar 1 1993
Gi0/1      5     0001.0000.d774  128.1.9.25      6  DHCP Deny   19:39:02 UTC
Mon Mar 1 1993
Gi0/1      5     0001.c940.1111  10.10.10.1      7  DHCP Deny   19:39:03 UTC
Mon Mar 1 1993
Gi0/1      5     0001.c940.1112  10.10.10.2      8  DHCP Deny   19:39:04 UTC
Mon Mar 1 1993
Gi0/1      5     0001.c940.1114  173.1.1.1      10  DHCP Deny   19:39:06 UTC
Mon Mar 1 1993
Gi0/1      5     0001.c940.1115  173.1.1.2      11  DHCP Deny   19:39:07 UTC
Mon Mar 1 1993
Gi0/1      5     0001.c940.1116  173.1.1.3      12  DHCP Deny   19:39:08 UTC
Mon Mar 1 1993
```

If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the **show ip arp inspection log** privileged EXEC command is affected. A -- in the display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer, or increase the logging rate in the **ip arp inspection log-buffer** global configuration command.

This is an example of output from the **show ip arp inspection statistics** command. It shows the statistics for packets that have been processed by dynamic ARP inspection for all active VLANs.

```
Switch# show ip arp inspection statistics
```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
5	3	4618	4605	4
2000	0	0	0	0
Vlan	DHCP Permits	ACL Permits	Source MAC Failures	
5	0	12	0	0
2000	0	0	0	0
Vlan	Dest MAC Failures	IP Validation Failures		
5	0	9		
2000	0	0		

For the **show ip arp inspection statistics** command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate failure count.

This is an example of output from the **show ip arp inspection statistics vlan 5** command. It shows statistics for packets that have been processed by dynamic ARP for VLAN 5.

Switch# show ip arp inspection statistics vlan 5				
Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
5	3	4618	4605	4
Vlan	DHCP Permits	ACL Permits	Source MAC Failures	
5	0	12	0	0
Vlan	Dest MAC Failures	IP Validation Failures		Invalid Protocol Data
5	0	9		3

This is an example of output from the **show ip arp inspection vlan 5** command. It shows the configuration and the operating state of dynamic ARP inspection for VLAN 5.

Switch# show ip arp inspection vlan 5					
Source Mac Validation	:Enabled	Destination Mac Validation	:Enabled	IP Address Validation	:Enabled
Vlan	Configuration	Operation	ACL Match	Static ACL	
5	Enabled	Active	second	No	
Vlan	ACL Logging	DHCP Logging			
5	Acl-Match	All			

## Related Commands

Command	Description
<a href="#">arp access-list</a>	Defines an ARP ACL.
<a href="#">clear ip arp inspection log</a>	Clears the dynamic ARP inspection log buffer.
<a href="#">clear ip arp inspection statistics</a>	Clears the dynamic ARP inspection statistics.
<a href="#">ip arp inspection log-buffer</a>	Configures the dynamic ARP inspection logging buffer.

■ **show ip arp inspection**

Command	Description
<b>ip arp inspection vlan logging</b>	Controls the type of packets that are logged per VLAN.
<b>show arp access-list</b>	Displays detailed information about ARP access lists.

# show ip dhcp snooping

Use the **show ip dhcp snooping** command in EXEC mode to display the DHCP snooping configuration.

**show ip dhcp snooping**

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Examples** This is an example of output from the **show ip dhcp snooping** command:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface           Trusted      Rate limit (pps)
-----              -----
```

## Related Commands

Command	Description
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.

---

 show ip dhcp snooping binding

# show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** command in EXEC mode to display the DHCP snooping binding database and configuration information for all interfaces on a switch.

**show ip dhcp snooping binding [ip-address] [mac-address] [interface interface-id] [vlan vlan-id]**

## Syntax Description

<i>ip-address</i>	(Optional) Specify the binding entry IP address.
<i>mac-address</i>	(Optional) Specify the binding entry MAC address.
<b>interface</b> <i>interface-id</i>	(Optional) Specify the binding input interface.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify the binding entry VLAN.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

### Usage Guidelines

The **show ip dhcp snooping binding** command output shows only the dynamically configured bindings. Use the **show ip source binding** privileged EXEC command to display the dynamically and statically configured bindings in the DHCP snooping binding database.

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

## Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch# show ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type        VLAN  Interface
-----  -----
01:02:03:04:05:06  10.1.2.150    9837      dhcp-snooping  20   GigabitEthernet0/1
00:D0:B7:1B:35:DE  10.1.2.151    237       dhcp-snooping  20   GigabitEthernet0/2
Total number of bindings: 2
```

This example shows how to display the DHCP snooping binding entries for a specific IP address:

```
Switch# show ip dhcp snooping binding 10.1.2.150
MacAddress      IpAddress      Lease(sec)  Type        VLAN  Interface
-----  -----
01:02:03:04:05:06  10.1.2.150    9810      dhcp-snooping  20   GigabitEthernet0/1
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries for a specific MAC address:

```
Switch# show ip dhcp snooping binding 0102.0304.0506
MacAddress          IpAddress        Lease(sec)   Type        VLAN  Interface
-----  -----  -----  -----  -----
01:02:03:04:05:06  10.1.2.150      9788        dhcp-snooping 20    GigabitEthernet0/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on a port:

```
Switch# show ip dhcp snooping binding interface gigabitethernet0/2
MacAddress          IpAddress        Lease(sec)   Type        VLAN  Interface
-----  -----  -----  -----  -----
00:30:94:C2:EF:35  10.1.2.151      290         dhcp-snooping 20    GigabitEthernet0/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on VLAN 20:

```
Switch# show ip dhcp snooping binding vlan 20
MacAddress          IpAddress        Lease(sec)   Type        VLAN  Interface
-----  -----  -----  -----  -----
01:02:03:04:05:06  10.1.2.150      9747        dhcp-snooping 20    GigabitEthernet0/1
00:00:00:00:00:02  10.1.2.151      65          dhcp-snooping 20    GigabitEthernet0/2
Total number of bindings: 2
```

[Table 2-35](#) describes the fields in the **show ip dhcp snooping binding** command output:

**Table 0-10      show ip dhcp snooping binding Command Output**

Field	Description
MacAddress	Client hardware MAC address
IpAddress	Client IP address assigned from the DHCP server
Lease(sec)	Remaining lease time for the IP address
Type	Binding type
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host
Total number of bindings	Total number of bindings configured on the switch <b>Note</b> The command output might not show the total number of bindings. For example, if 200 bindings are configured on the switch and you stop the display before all the bindings appear, the total number does not change.

#### Related Commands

Command	Description
<a href="#">ip dhcp snooping binding</a>	Configures the DHCP snooping binding database
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.

---

■ show ip dhcp snooping database

# show ip dhcp snooping database

Use the **show ip dhcp snooping database** command in EXEC mode to display the status of the DHCP snooping binding database agent.

**show ip dhcp snooping database [detail]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed status and statistics information.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Examples

This is an example of output from the **show ip dhcp snooping database** command:

```
Switch# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts : 0 Startup Failures : 0
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
Media Failures : 0
```

This is an example of output from the **show ip dhcp snooping database detail** command:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts : 21 Startup Failures : 0
Successful Transfers : 0 Failed Transfers : 21
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 21
Media Failures : 0
```

```
First successful access: Read

Last ignored bindings counters :
Binding Collisions      :      0    Expired leases      :      0
Invalid interfaces       :      0    Unsupported vlans :      0
Parse failures          :      0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions      :      0    Expired leases      :      0
Invalid interfaces       :      0    Unsupported vlans :      0
Parse failures          :      0
```

**Related Commands**

Command	Description
<a href="#">ip dhcp snooping</a>	Enables DHCP snooping on a VLAN.
<a href="#">ip dhcp snooping database</a>	Configures the DHCP snooping binding database agent or the binding file.
<a href="#">show ip dhcp snooping</a>	Displays DHCP snooping information.

---

```
■ show ip dhcp snooping statistics
```

# show ip dhcp snooping statistics

Use the **show ip dhcp snooping statistics** command in EXEC mode to display DHCP snooping statistics in summary or detail form.

**show ip dhcp snooping statistics [detail]**

<b>Syntax Description</b>	<b>detail</b>	(Optional) Display detailed statistics information.
---------------------------	---------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(37)SE	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show ip dhcp snooping statistics</b> command:
-----------------	--

```
Switch# show ip dhcp snooping statistics
Packets Forwarded = 0
Packets Dropped = 0
Packets Dropped From untrusted ports = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Switch# show ip dhcp snooping statistics detail
Packets Processed by DHCP Snooping = 0
Packets Dropped Because
    IDB not known = 0
    Queue full = 0
    Interface is in errdisabled = 0
    Rate limit exceeded = 0
    Received on untrusted ports = 0
    Nonzero giaddr = 0
    Source mac not equal to chaddr = 0
    Binding mismatch = 0
    Insertion of opt82 fail = 0
    Interface Down = 0
    Unknown output interface = 0
    Reply output port equal to input port = 0
    Packet denied by platform = 0
```

[Table 2-36](#) shows the DHCP snooping statistics and their descriptions:

**Table 0-11      DHCP Snooping Statistics**

<b>DHCP Snooping Statistic</b>	<b>Description</b>
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.

**Table 0-11      DHCP Snooping Statistics (continued)**

DHCP Snooping Statistic	Description
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the <b>no ip dhcp snooping information option allow-untrusted</b> global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the <b>ip dhcp snooping verify mac-address</b> global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

**Related Commands**

■ show ip dhcp snooping statistics

Command	Description
<b>clear ip dhcp snooping</b>	Clears the DHCP snooping binding database, the DHCP snooping binding database agent statistics, or the DHCP snooping statistics counters.

# show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

**show ip igmp profile [profile number]**

<b>Syntax Description</b>	<i>profile number</i> (Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.
---------------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

**Examples** These are examples of output from the **show ip igmp profile** privileged EXEC command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
    range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
    range 229.9.9.0 229.255.255.255
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ip igmp profile</a>	Configures the specified IGMP profile number.

---

```
■ show ip igmp snooping
```

# show ip igmp snooping

Use the **show ip igmp snooping** command in EXEC mode to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

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

## Syntax Description

<b>groups</b>	(Optional) See the <a href="#">show ip igmp snooping groups</a> command.
<b>mrouter</b>	(Optional) See the <a href="#">show ip igmp snooping mrouter</a> command.
<b>querier</b>	(Optional) See the <a href="#">show ip igmp snooping querier</a> command.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).

## Command Modes

User EXEC  
Privileged EXEC

## Command History

### Usage Guidelines

Use this command to display snooping configuration for the switch or for a specific VLAN.

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

## Examples

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

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----
IGMP snooping :Enabled
IGMPv3 snooping (minimal) :Enabled
Report suppression :Enabled
TCN solicit query :Disabled
TCN flood query count :2
Last member query interval : 100

Vlan 1:
-----
IGMP snooping :Enabled
Immediate leave :Disabled
Multicast router learning mode :pim-dvmrp
Source only learning age timer :10
CGMP interoperability mode :IGMP_ONLY
Last member query interval : 100
```

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

```
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping : Enabled
```

```

IGMPv3 snooping (minimal) : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count    : 2
Last member query interval : 100

Vlan 1:
-----
IGMP snooping           : Enabled
Immediate leave          : Disabled
Multicast router learning mode : pim-dvmrp
Source only learning age timer : 10
CGMP interoperability mode : IGMP_ONLY
Last member query interval : 100

Vlan 2:
-----
IGMP snooping           : Enabled
Immediate leave          : Disabled
Multicast router learning mode : pim-dvmrp
Source only learning age timer : 10
CGMP interoperability mode : IGMP_ONLY
Last member query interval : 333

<output truncated>

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>ip igmp snooping</b></a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#"><b>ip igmp snooping last-member-query-interval</b></a>	Enables the IGMP snooping configurable-leave timer.
<a href="#"><b>ip igmp snooping querier</b></a>	Enables the IGMP querier function in Layer 2 networks.
<a href="#"><b>ip igmp snooping report-suppression</b></a>	Enables IGMP report suppression.
<a href="#"><b>ip igmp snooping tcn</b></a>	Configures the IGMP topology change notification behavior.
<a href="#"><b>ip igmp snooping tcn flood</b></a>	Specifies multicast flooding as the IGMP spanning-tree topology change notification behavior.
<a href="#"><b>ip igmp snooping vlan immediate-leave</b></a>	Enables IGMP snooping immediate-leave processing on a VLAN.
<a href="#"><b>ip igmp snooping vlan mrouter</b></a>	Adds a multicast router port or configures the multicast learning method.
<a href="#"><b>ip igmp snooping vlan static</b></a>	Statically adds a Layer 2 port as a member of a multicast group.
<a href="#"><b>show ip igmp snooping groups</b></a>	Displays the IGMP snooping multicast table for the switch.
<a href="#"><b>show ip igmp snooping mrouter</b></a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
<a href="#"><b>show ip igmp snooping querier</b></a>	Displays the configuration and operation information for the IGMP querier configured on a switch.

---

 show ip igmp snooping groups
 

---

# show ip igmp snooping groups

Use the **show ip igmp snooping groups** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information. Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or specific multicast information.

**show ip igmp snooping groups [count] [dynamic] [user] [vlan *vlan-id*] [*ip\_address*]]**

<b>Syntax Description</b>	<b>count</b> (Optional) Display the total number of entries for the specified command options instead of the actual entries. <b>dynamic</b> (Optional) Display entries learned by IGMP snooping. <b>user</b> (Optional) Display only the user-configured multicast entries. <b>vlan <i>vlan-id</i></b> (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. <b><i>ip_address</i></b> (Optional) Display characteristics of the multicast group with the specified group IP address.
---------------------------	--

---

**Command Modes** Privileged EXEC

---

**Command History**

---

**Usage Guidelines**

Use this command to display multicast information or the multicast table.

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

---

**Examples**

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

```
Switch# show ip igmp snooping groups
Vlan      Group          Type      Version      Port List
-----
```

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

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

This is an example of output from the **show ip igmp snooping groups dynamic** command. It shows only the entries learned by IGMP snooping.

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group          Type      Version      Port List
-----
```

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

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group          Type      Version      Port List
```

Related Commands	Command	Description
	<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
	<a href="#">ip igmp snooping vlan mrouter</a>	Configures a multicast router port.
	<a href="#">ip igmp snooping vlan static</a>	Statically adds a Layer 2 port as a member of a multicast group.
	<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN.
	<a href="#">show ip igmp snooping mrouter</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

---

■ **show ip igmp snooping mrouter**

## show ip igmp snooping mrouter

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

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

---

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
---------------------------	--

---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

---

### Command History

**Usage Guidelines** Use this command to display multicast router ports on the switch or for a specific VLAN.

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

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

---

### Examples

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

```
Switch# show ip igmp snooping mrouter
```

---

### Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#">ip igmp snooping vlan mrouter</a>	Adds a multicast router port.
<a href="#">ip igmp snooping vlan static</a>	Statically adds a Layer 2 port as a member of a multicast group.
<a href="#">show ip igmp snooping</a>	Displays the IGMP snooping configuration of the switch or the VLAN
<a href="#">show ip igmp snooping groups</a>	Displays IGMP snooping multicast information for the switch or for the specified parameter.

---

# show ip igmp snooping querier

Use the **show ip igmp snooping querier detail** command in EXEC mode to display the configuration and operation information for the IGMP querier configured on a switch.

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

<b>Syntax Description</b>	<b>detail</b> Optional) Display detailed IGMP querier information. <b>vlan <i>vlan-id</i> [detail]</b> Optional) Display IGMP querier information for the specified VLAN. The range is 1 to 1001 and 1006 to 4094. Use the <b>detail</b> keyword to display detailed information.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

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

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

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

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

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

## Examples

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

```
Switch# show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11    v3                  Gi0/1
2         172.20.40.20    v2                  Router
```

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

```
Switch# show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1          v2                  Fa0/1
```

■ **show ip igmp snooping querier**

```
Global IGMP switch querier status
-----
admin state          : Enabled
admin version       : 2
source IP address   : 0.0.0.0
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count     : 2
tcn query interval (sec) : 10

Vlan 1:    IGMP switch querier status
-----
selected querier is 1.1.1.1      on port Fa0/1
-----
admin state          : Enabled
admin version       : 2
source IP address   : 10.1.1.65
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count     : 2
tcn query interval (sec) : 10
operational state   : Non-Querier
operational version : 2
tcn query pending count : 0
```

#### Related Commands

Command	Description
<a href="#">ip igmp snooping</a>	Enables IGMP snooping on the switch or on a VLAN.
<a href="#">ip igmp snooping querier</a>	Enables the IGMP querier function in Layer 2 networks.
<a href="#">show ip igmp snooping</a>	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

# show ip source binding

Use the **show ip source binding** command in EXEC mode to display the IP source bindings on the switch.

```
show ip source binding [ip-address] [mac-address] [dhcp-snooping | static] [interface interface-id] [vlan vlan-id]
```

<b>Syntax Description</b>	
<i>ip-address</i>	(Optional) Display IP source bindings for a specific IP address.
<i>mac-address</i>	(Optional) Display IP source bindings for a specific MAC address.
<b>dhcp-snooping</b>	(Optional) Display IP source bindings that were learned by DHCP snooping.
<b>static</b>	(Optional) Display static IP source bindings.
<b>interface <i>interface-id</i></b>	(Optional) Display IP source bindings on a specific interface.
<b>vlan <i>vlan-id</i></b>	(Optional) Display IP source bindings on a specific VLAN.

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

**Usage Guidelines** The **show ip source binding** command output shows the dynamically and statically configured bindings in the DHCP snooping binding database.

Use the **show ip dhcp snooping binding** privileged EXEC command to display only the dynamically configured bindings.

**Examples** This is an example of output from the **show ip source binding** command:

```
Switch# show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN   Interface
-----              -----            -----       -----         -----   -----
00:00:00:0A:00:0B  11.0.0.1        infinite    static        10     GigabitEthernet0/1
00:00:00:0A:00:0A  11.0.0.2        10000      dhcp-snooping 10     GigabitEthernet0/1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>ip dhcp snooping binding</b></a>	Configures the DHCP snooping binding database.
	<a href="#"><b>ip source binding</b></a>	Configures static IP source bindings on the switch.

**show ip verify source**

# show ip verify source

Use the **show ip verify source** command in EXEC mode to display the IP source guard configuration on the switch or on a specific interface.

**show ip verify source [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b> (Optional) Display IP source guard configuration on a specific interface.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	
------------------------	--

<b>Examples</b>	This is an example of output from the <b>show ip verify source</b> command:
-----------------	---

```
Switch# show ip verify source
Interface Filter-type Filter-mode IP-address Mac-address Vlan
----- ----- ----- ----- ----- -----

```

In the previous example, this is the IP source guard configuration:

- On the Gigabit Ethernet 1 interface, DHCP snooping is enabled on VLANs 10 to 20. For VLAN 10, IP source guard with IP address filtering is configured on the interface, and a binding exists on the interface. For VLANs 11 to 20, the second entry shows that a default port access control lists (ACLs) is applied on the interface for the VLANs on which IP source guard is not configured.
- The Gigabit Ethernet 2 interface is configured as trusted for DHCP snooping.
- On the Gigabit Ethernet 3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.
- On the Gigabit Ethernet 4 interface, IP source guard with source IP and MAC address filtering is enabled, and static IP source bindings are configured on VLANs 10 and 11. For VLANs 12 to 20, the default port ACL is applied on the interface for the VLANs on which IP source guard is not configured.
- On the Gigabit Ethernet 5 interface, IP source guard with source IP and MAC address filtering is enabled and configured with a static IP binding, but port security is disabled. The switch cannot filter source MAC addresses.

This is an example of output on an interface on which IP source guard is disabled:

```
Switch# show ip verify source gigabitethernet
IP source guard is not configured on the interface gi0/6.
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>ip verify source</b></a>	Enables IP source guard on an interface.



Note

# show ipv6 mld snooping

Use the **show ipv6 mld snooping** command in EXEC mode to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

**show ipv6 mld snooping [vlan *vlan-id*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
<b>Command Modes</b>	User EXEC Privileged EXEC
<b>Command History</b>	
<b>Usage Guidelines</b>	<p>Use this command to display MLD snooping configuration for the switch or for a specific VLAN. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.</p> <p>To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6</b> global configuration command and reload the switch.</p>
<b>Examples</b>	<p>This is an example of output from the <b>show ipv6 mld snooping vlan</b> command. It shows snooping characteristics for a specific VLAN.</p> <pre>Switch# show ipv6 mld snooping vlan 100 Global MLD Snooping configuration: ----- MLD snooping : Enabled MLDv2 snooping (minimal) : Enabled Listener message suppression : Enabled TCN solicit query : Disabled TCN flood query count : 2 Robustness variable : 3 Last listener query count : 2 Last listener query interval : 1000 Vlan 100: ----- MLD snooping : Disabled MLDv1 immediate leave : Disabled Explicit host tracking : Enabled Multicast router learning mode : pim-dvmrp Robustness variable : 3 Last listener query count : 2 Last listener query interval : 1000</pre> <p>This is an example of output from the <b>show ipv6 mld snooping</b> command. It displays snooping characteristics for all VLANs on the switch.</p> <pre>Switch# show ipv6 mld snooping Global MLD Snooping configuration: ----- MLD snooping : Enabled MLDv2 snooping (minimal) : Enabled</pre>

show ipv6 mld snooping

```

Listener message suppression : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Robustness variable        : 3
Last listener query count  : 2
Last listener query interval: 1000

Vlan 1:
-----
MLD snooping                : Disabled
MLDv1 immediate leave        : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode: pim-dvmrp
Robustness variable          : 1
Last listener query count    : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-----
MLD snooping                : Disabled
MLDv1 immediate leave        : Disabled
Explicit host tracking       : Enabled
Multicast router learning mode: pim-dvmrp
Robustness variable          : 3
Last listener query count    : 2
Last listener query interval : 1000

```

#### Related Commands

Command	Description
<a href="#">ipv6 mld snooping</a>	Enables and configures MLD snooping on the switch or on a VLAN.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 mld snooping address

Use the **show ipv6 mld snooping address** command in EXEC mode to display all or specified IP version 6 (IPv6) multicast address information maintained by Multicast Listener Discovery (MLD) snooping.

```
show ipv6 mld snooping address [[vlan vlan-id] [ipv6 address]] [vlan vlan-id] [count | dynamic | user]
```

<b>Syntax Description</b>	
<b>vlan vlan-id</b>	(Optional) Specify a VLAN about which to show MLD snooping multicast address information. The VLAN ID range is 1 to 1001 and 1006 to 4094.
<i>ipv6-multicast-address</i>	(Optional) Display information about the specified IPv6 multicast address. This keyword is only available when a VLAN ID is entered.
<b>count</b>	(Optional) Display the number of multicast groups on the switch or in the specified VLAN.
<b>dynamic</b>	(Optional) Display MLD snooping learned group information.
<b>user</b>	(Optional) Display MLD snooping user-configured group information.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

### Usage Guidelines

Use this command to display IPv6 multicast address information.

You can enter an IPv6 multicast address only after you enter a VLAN ID.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

Use the **dynamic** keyword to display information only about groups that are learned. Use the **user** keyword to display information only about groups that have been configured.

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6** global configuration command and reload the switch.

## Examples

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

```
Switch# show ipv6 mld snooping address
Vlan Group      Type Version Port List
-----
```

This is an example of output from the **show snooping address count** command:

```
Switch# show ipv6 mld snooping address count
Total number of multicast groups: 2
```

This is an example of output from the **show snooping address user** command:

```
Switch# show ipv6 mld snooping address user
Vlan Group      Type Version Port List
```

show ipv6 mld snooping address

---

**Related Commands**

Command	Description
<a href="#">ipv6 mld snooping vlan</a>	Configures IPv6 MLD snooping on a VLAN.
<a href="#">sdm prefer</a>	Configures an SDM template to optimize system resources based on how the switch is being used.

---

# show ipv6 mld snooping mrouter

Use the **show ipv6 mld snooping mrouter** command in EXEC mode to display dynamically learned and manually configured IP version 6 (IPv6) Multicast Listener Discovery (MLD) router ports for the switch or a VLAN.

**show ipv6 mld snooping mrouter [vlan *vlan-id*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b>	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
---------------------------	----------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SED	This command was introduced.

<b>Usage Guidelines</b>	Use this command to display MLD snooping router ports for the switch or for a specific VLAN.  VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.  To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6</b> global configuration command and reload the switch.
-------------------------	---

<b>Examples</b>	This is an example of output from the <b>show ipv6 mld snooping mrouter</b> command. It displays snooping characteristics for all VLANs on the switch that are participating in MLD snooping.
-----------------	---

```
Switch# show ipv6 mld snooping mrouter
Vlan      ports
----      -----

```

This is an example of output from the **show ipv6 mld snooping mrouter vlan** command. It shows multicast router ports for a specific VLAN.

```
Switch# show ipv6 mld snooping mrouter vlan 100
Vlan      ports
----      -----
2        Gi0/11 (dynamic)
```

show ipv6 mld snooping mrouter

#### Related Commands

Command	Description
<b>ipv6 mld snooping</b>	Enables and configures MLD snooping on the switch or on a VLAN.
<b>ipv6 mld snooping vlan mrouter interface</b> <i>interface-id</i>   static <i>ipv6-multicast-address</i> <b>interface</b> <i>interface-id</i>	Configures multicast router ports for a VLAN.
<b>sdm prefer</b>	Configures an SDM template to optimize system resources based on how the switch is being used.

# show ipv6 mld snooping querier

Use the **show ipv6 mld snooping querier** command in EXEC mode to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping querier-related information most recently received by the switch or the VLAN.

**show ipv6 mld snooping querier [vlan *vlan-id*] [detail]**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. <b>detail</b> (Optional) Display MLD snooping detailed querier information for the switch or for the VLAN.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

<b>Usage Guidelines</b>	<p>Use the <b>show ipv6 mld snooping querier</b> command to display the MLD version and IPv6 address of a detected device that sends MLD query messages, which is also called a <i>querier</i>. A subnet can have multiple multicast routers but has only one MLD querier. The querier can be a Layer 3 switch.</p> <p>The <b>show ipv6 mld snooping querier</b> command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the <i>Port</i> field as <i>Router</i>. If the querier is a router, the output shows the port number on which the querier is learned in the <i>Port</i> field.</p> <p>The output of the <b>show ipv6 mld snoop querier vlan</b> command displays the information received in response to a query message from an external or internal querier. It does not display user-configured VLAN values, such as the snooping robustness variable on the particular VLAN. This querier information is used only on the MASQ message that is sent by the switch. It does not override the user-configured robustness variable that is used for aging out a member that does not respond to query messages.</p> <p>VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.</p> <p>To configure the dual IPv4 and IPv6 template, enter the <b>sdm prefer dual-ipv4-and-ipv6</b> global configuration command and reload the switch.</p>
-------------------------	---

■ **show ipv6 mld snooping querier**

**Examples**

This is an example of output from the **show ipv6 mld snooping querier** command:

```
Switch# show ipv6 mld snooping querier
Vlan      IP Address          MLD Version Port
-----
2        FE80::201:C9FF:FE40:6000 v1           Gi0/1
```

This is an example of output from the **show ipv6 mld snooping querier detail** command:

```
Switch# show ipv6 mld snooping querier detail
Vlan      IP Address          MLD Version Port
-----
2        FE80::201:C9FF:FE40:6000 v1           Gi0/1
```

This is an example of output from the **show ipv6 mld snooping querier vlan** command:

```
Switch# show ipv6 mld snooping querier vlan 2
IP address : FE80::201:C9FF:FE40:6000
MLD version : v1
Max response time : 1000s
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>ipv6 mld snooping</b></a>	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.
<a href="#"><b>ipv6 mld snooping last-listener-query-count</b></a>	Configures the maximum number of queries that the switch sends before aging out an MLD client.
<a href="#"><b>ipv6 mld snooping last-listener-query-interval</b></a>	Configures the maximum response time after sending out a query that the switch waits before deleting a port from the multicast group.
<a href="#"><b>ipv6 mld snooping robustness-variable</b></a>	Configures the maximum number of queries that the switch sends before aging out a multicast address when there is no response.
<a href="#"><b>sdm prefer</b></a>	Configures an SDM template to optimize system resources based on how the switch is being used.
<a href="#"><b>ipv6 mld snooping</b></a>	Enables and configures IPv6 MLD snooping on the switch or on a VLAN.

# show ipv6 route updated

Use the **show ipv6 route updated** command in EXEC mode to display the current contents of the IPv6 routing table.

```
show ipv6 route [protocol] updated [boot-up]{hh:mm | day{month [hh:mm]} } [{hh:mm | day{month [hh:mm]} }]
```

<b>Syntax Description</b>	<p><i>protocol</i> (Optional) Displays routes for the specified routing protocol using any of these keywords:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b></li> <li>• <b>isis</b></li> <li>• <b>ospf</b></li> <li>• <b>rip</b></li> </ul> <p>or displays routes for the specified type of route using any of these keywords:</p> <ul style="list-style-type: none"> <li>• <b>connected</b></li> <li>• <b>local</b></li> <li>• <b>static</b></li> <li>• <b>interface <i>interface id</i></b></li> </ul>
<b>boot-up</b>	Display the current contents of the IPv6 routing table.
<i>hh:mm</i>	Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:). For example, enter <b>13:32</b>
<i>day</i>	Enter the day of the month. The range is from 1 to 31.
<i>month</i>	Enter the month in upper case or lower case letters. You can enter the full name of the month, such as <b>January</b> or <b>august</b> , or the first three letters of the month, such as <b>jan</b> or <b>Aug</b> .

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

**Usage Guidelines** Use the **show ipv6 route** privileged EXEC command to display the current contents of the IPv6 routing table.

**show ipv6 route updated****Examples**

This is an example of output from the **show ipv6 route updated rip** command.

```
Switch# show ipv6 route rip updated
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
IA - ISIS interarea, IS - ISIS summary
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R 2001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:8D01, GigabitEthernet0/1
Last updated 10:31:10 27 February 2007
R 2004::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/2
Last updated 17:23:05 22 February 2007
R 4000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/3
Last updated 17:23:05 22 February 2007
R 5000::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/4
Last updated 17:23:05 22 February 2007
R 5001::/64 [120/2]
via FE80::A8BB:CCFF:FE00:9001, GigabitEthernet0/5
Last updated 17:23:05 22 February 2007
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ipv6 route</b>	Displays the current contents of the IPv6 routing table.

# show lacp

Use the **show lacp** command in EXEC mode to display Link Aggregation Control Protocol (LACP) channel-group information.

**show lacp [channel-group-number] {counters | internal | neighbor | sys-id}**

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to .
<b>counters</b>	Display traffic information.
<b>internal</b>	Display internal information.
<b>neighbor</b>	Display neighbor information.
<b>sys-id</b>	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

### Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

## Examples

This is an example of output from the **show lacp counters** command. [Table 2-38](#) describes the fields in the display.

```
Switch# show lacp counters
      LACPDUs          Marker          Marker Response    LACPDUs
Port     Sent     Recv     Sent     Recv     Sent     Recv     Pkts Err
-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+-----+
Channel group:1
```

**Table 0-12      show lacp counters Field Descriptions**

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

**show lacp**

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

```
Switch# show lacp 1 internal
Flags: S - Device is requesting Slow LACPDU
      F - Device is requesting Fast LACPDU
      A - Device is in Active mode          P - Device is in Passive mode

Channel group 1
Port     Flags   State       LACP port    Admin Key   Oper Key   Port Number   Port State

```

[Table 2-39](#) describes the fields in the display:

**Table 0-13      *show lacp internal* Field Descriptions**

Field	Description
State	<p>State of the specific port. These are the allowed values:</p> <ul style="list-style-type: none"> <li>• ——Port is in an unknown state.</li> <li>• <b>bndl</b>—Port is attached to an aggregator and bundled with other ports.</li> <li>• <b>susp</b>—Port is in a suspended state; it is not attached to any aggregator.</li> <li>• <b>hot-sby</b>—Port is in a hot-standby state.</li> <li>• <b>indiv</b>—Port is incapable of bundling with any other port.</li> <li>• <b>indep</b>—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).</li> <li>• <b>down</b>—Port is down.</li> </ul>
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.

**Table 0-13** show lacp internal Field Descriptions (continued)

Field	Description
Port Number	Port number.
Port State	<p>State variables for the port, encoded as individual bits within a single octet with these meanings:</p> <ul style="list-style-type: none"> <li>• bit0: LACP_Activity</li> <li>• bit1: LACP_Timeout</li> <li>• bit2: Aggregation</li> <li>• bit3: Synchronization</li> <li>• bit4: Collecting</li> <li>• bit5: Distributing</li> <li>• bit6: Defaulted</li> <li>• bit7: Expired</li> </ul> <p><b>Note</b> In the list above, bit7 is the MSB and bit0 is the LSB.</p>

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

```
Switch# show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode      P - Device is in Passive mode
```

Channel group 3 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

Partner's information:

Port	Partner System ID	Partner Port Number	Age	Partner Flags
	LACP Partner	Partner	Partner	
	Port Priority	Oper Key	Port State	
	32768	0x3	0x3C	

This is an example of output from the **show lacp sys-id** command:

```
Switch# show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

**show lacp****Related Commands**

Command	Description
<a href="#">clear lacp</a>	Clears the LACP channel-group information.
<a href="#">lacp port-priority</a>	Configures the LACP port priority.
<a href="#">lacp system-priority</a>	Configures the LACP system priority.

# show link state group

Use the **show link state group** privileged EXEC command to display the link-state group information.

**show link state group [number] [detail]**

<b>Syntax Description</b>	<b>number</b> (Optional) Number of the link-state group.
	<b>detail</b> (Optional) Specify that detailed information appears.

<b>Defaults</b>	There is no default.
-----------------	----------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEE	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show link state group</b> command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group.
-------------------------	--

Enter the **detail** keyword to display detailed information about the group. The output for the **show link state group detail** command displays only those link-state groups that have link-state tracking enabled or that have upstream or downstream interfaces (or both) configured. If there is no link-state group configuration for a group, it is not shown as enabled or disabled.

<b>Examples</b>	This is an example of output from the <b>show link state group 1</b> command:
-----------------	---

```
Switch# show link state group 1
Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the **show link state group detail** command:

```
Switch# show link state group detail
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down

Link State Group: 2 Status: Enabled, Down

(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled
```

<b>Related Commands</b>
-------------------------

■ show link state group

Command	Description
<b>link state group</b>	Configures an interface as a member of a link-state group.
<b>link state track</b>	Enables a link-state group.
<b>show running-config</b>	Displays the current operating configuration.

# show location

Use the **show location** command in EXEC mode to display location information for an endpoint.

**show location admin-tag**

**show location civic-location {identifier *id number* | interface *interface-id* | static}**

**show location elin-location {identifier *id number* | interface *interface-id* | static}**

Syntax Description	
<b>admin-tag</b>	Display administrative tag or site information.
<b>civic-location</b>	Display civic location information.
<b>elin-location</b>	Display emergency location information (ELIN).
<b>identifier <i>id</i></b>	Specify the ID for the civic location or the elin location. The id range is 1 to 4095.
<b>interface <i>interface-id</i></b>	(Optional) Display location information for the specified interface or all interfaces. Valid interfaces include physical ports.
<b>static</b>	Display static configuration information.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

## Usage Guidelines

Use the **show location** command to display location information for an endpoint.

## Examples

This is an example of output from the **show location civic-location** command that displays location information for an interface:

```
Switch# show location civic interface gigabitethernet
Civic location information
-----
Identifier : 1
County : Santa Clara
Street number : 3550
Building : 19
Room : C6
Primary road name : Cisco Way
City : San Jose
State : CA
Country : US
```

This is an example of output from the **show location civic-location static** command that displays all the civic location information:

```
Switch# show location civic-location static
Civic location information
-----
Identifier : 1
```

**show location**

```

County : Santa Clara
Street number : 3550
Building : 19
Room : C6
Primary road name : Cisco Way
City : San Jose
State : CA
Country : US
Ports : Gi0/1
-----
Identifier : 2
Street number : 24568
Street number suffix : West
Landmark : Golden Gate Bridge
Primary road name : 19th Ave
City : San Francisco
Country : US
-----
```

This is an example of output from the **show location elin-location** command that displays the emergency location information:

```

Switch# show location elin-location identifier 1
Elin location information
-----
Identifier : 1
Elin : 14085553881
Ports : Gi0/2
```

This is an example of output from the **show location elin static** command that displays all emergency location information:

```

Switch# show location elin static
Elin location information
-----
Identifier : 1
Elin : 14085553881
Ports : Gi0/2
-----
Identifier : 2
Elin : 18002228999
-----
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>location (global configuration)</b></a>	Configures the global location information for an endpoint.
<a href="#"><b>location (interface configuration)</b></a>	Configures the location information for an interface.

# show mac access-group

Use the **show mac access-group** command in EXEC mode to display the MAC access control lists (ACLs) configured for an interface or a switch.

**show mac access-group [interface *interface-id*]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b>	(Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to (available only in privileged EXEC mode).
---------------------------	--------------------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Examples

This is an example of output from the **show mac-access group** command. Port 2 has the MAC access list *macl\_e1* applied; no MAC ACLs are applied to other interfaces.

```
Switch# show mac access-group
Interface GigabitEthernet0/1:
    Inbound access-list is not set
Interface GigabitEthernet0/2:
    Inbound access-list is macl_e1
Interface GigabitEthernet0/3:
    Inbound access-list is not set
Interface GigabitEthernet0/4:
    Inbound access-list is not set

<output truncated>
```

This is an example of output from the **show mac access-group interface** command:

```
Switch# show mac access-group interface gigabitethernet0/1
Interface GigabitEthernet0/1:
    Inbound access-list is macl_e1
```

### Related Commands

Command	Description
<a href="#">mac access-group</a>	Applies a MAC access group to an interface.

---

 show mac address-table
 

---

# show mac address-table

Use the **show mac address-table** command in EXEC mode to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

## show mac address-table

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

**Command Modes** User EXEC  
Privileged EXEC

**Command History**

**Examples** This is an example of output from the **show mac address-table** command:

```
Switch# show mac address-table
      Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
A11    0000.0000.0001    STATIC    CPU
A11    0000.0000.0002    STATIC    CPU
A11    0000.0000.0003    STATIC    CPU
A11    0000.0000.0009    STATIC    CPU
A11    0000.0000.0012    STATIC    CPU
A11    0180.c200.000b    STATIC    CPU
A11    0180.c200.000c    STATIC    CPU
A11    0180.c200.000d    STATIC    CPU
A11    0180.c200.000e    STATIC    CPU
A11    0180.c200.000f    STATIC    CPU
A11    0180.c200.0010    STATIC    CPU
      1  0030.9441.6327    DYNAMIC   Gi0/4
Total Mac Addresses for this criterion: 12
```

Related Commands	Command	Description
	<a href="#">clear mac address-table dynamic</a>	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
	<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
	<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.

Command	Description
<b>show mac address-table static</b>	Displays static MAC address table entries only.
<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

---

 show mac address-table address
 

---

# show mac address-table address

Use the **show mac address-table address** command in EXEC mode to display MAC address table information for the specified MAC address.

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

Syntax Description	<i>mac-address</i> Specify the 48-bit MAC address; the valid format is H.H.H. <b>interface</b> <i>interface-id</i> (Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels. <b>vlan</b> <i>vlan-id</i> (Optional) Display entries for the specific VLAN only. The range is 1 to 4094.
--------------------	--

---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

---

## Command History

### Examples

This is an example of output from the **show mac address-table address** command:

```
Switch# show mac address-table address 0002.4b28.c482
      Mac Address Table
-----
Vlan      Mac Address          Type      Ports
----      -----
All      0002.4b28.c482    STATIC    CPU
Total Mac Addresses for this criterion: 1
```

---

Related Commands	Command	Description
	<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
	<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.
	<a href="#">show mac address-table vlan</a>	Displays the MAC address table information for the specified VLAN.

---

# show mac address-table aging-time

Use the **show mac address-table aging-time** command in EXEC mode to display the aging time of a specific address table instance, all address table instances on a specified VLAN or, if a specific VLAN is not specified, on all VLANs.

**show mac address-table aging-time [vlan *vlan-id*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Display aging time information for a specific VLAN. The range is 1 to 4094.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

If no VLAN number is specified, the aging time for all VLANs appears.

## Examples

This is an example of output from the **show mac address-table aging-time** command:

```
Switch# show mac address-table aging-time
Vlan      Aging Time
---      -----
1          300
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch# show mac address-table aging-time vlan 10
Vlan      Aging Time
---      -----
10         300
```

■ **show mac address-table aging-time**

Related Commands	Command	Description
	<b>mac address-table aging-time</b>	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
	<b>show mac address-table address</b>	Displays MAC address table information for the specified MAC address.
	<b>show mac address-table count</b>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<b>show mac address-table dynamic</b>	Displays dynamic MAC address table entries only.
	<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
	<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<b>show mac address-table static</b>	Displays static MAC address table entries only.
	<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

# show mac address-table count

Use the **show mac address-table count** command in EXEC mode to display the number of addresses present in all VLANs or the specified VLAN.

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

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

If no VLAN number is specified, the address count for all VLANs appears.

## Examples

This is an example of output from the **show mac address-table count** command:

```
Switch# show mac address-table count
Mac Entries for Vlan : 1
-----
Dynamic Address Count : 2
Static Address Count : 0
Total Mac Addresses : 2
```

## Related Commands

Command	Description
<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.
<a href="#">show mac address-table vlan</a>	Displays the MAC address table information for the specified VLAN.

---

 show mac address-table dynamic
 

---

# show mac address-table dynamic

Use the **show mac address-table dynamic** command in EXEC mode to display only dynamic MAC address table entries.

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

<b>Syntax Description</b>	<b>address mac-address</b> (Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
<b>interface interface-id</b>	(Optional) Specify an interface to match; valid <i>interfaces</i> include physical ports and port channels.
<b>vlan vlan-id</b>	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Examples

This is an example of output from the **show mac address-table dynamic** command:

```
Switch# show mac address-table dynamic
      Mac Address Table
-----
Vlan      Mac Address          Type      Ports
----      -----
  1      0030.b635.7862    DYNAMIC   Gi0/2
  1      00b0.6496.2741    DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 2
```

Related Commands	Command	Description
	<a href="#">clear mac address-table dynamic</a>	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
	<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
	<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.
	<a href="#">show mac address-table vlan</a>	Displays the MAC address table information for the specified VLAN.

# show mac address-table interface

Use the **show mac address-table interface** user command to display the MAC address table information for the specified interface in the specified VLAN.

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

<b>Syntax Description</b>	<i>interface-id</i> Specify an interface type; valid interfaces include physical ports and port channels. <b>vlan <i>vlan-id</i></b> (Optional) Display entries for a specific VLAN; the range is 1 to 4094.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Examples

This is an example of output from the **show mac address-table interface** command:

```
Switch# show mac address-table interface gigabitethernet0/2
      Mac Address Table
-----
Vlan      Mac Address          Type      Ports
----      -----
  1      0030.b635.7862    DYNAMIC   Gi0/2
  1      00b0.6496.2741    DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
	<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.
	<a href="#">show mac address-table vlan</a>	Displays the MAC address table information for the specified VLAN.

---

show mac address-table learning

# show mac address-table learning

Use the **show mac address-table learning** command in EXEC mode to display the status of MAC address learning for all VLANs or the specified VLAN.

**show mac address-table learning [vlan *vlan-id*]**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b>	(Optional) Display information for a specific VLAN. The range is 1 to 4094.
---------------------------	----------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(46)SE1	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show mac address-table learning</b> command without any keywords to display configured VLANs and whether MAC address learning is enabled or disabled on them. The default is that MAC address learning is enabled on all VLANs. Use the command with a specific VLAN ID to display the learning status on an individual VLAN.
-------------------------	--

<b>Examples</b>	This is an example of output from the <b>show mac address-table learning</b> command showing that MAC address learning is disabled on VLAN 200:
	<pre>Switch# show mac address-table learning VLAN      Learning Status ---      ----- 1          yes 100        yes 200        no</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>mac address-table learning vlan</b></a>	Enables or disables MAC address learning on a VLAN.

# show mac address-table move update

Use the **show mac address-table move update** command in EXEC mode to display the MAC address-table move update information on the switch.

## show mac address-table move update

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

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	12.2(25)SED	This command was introduced.

**Examples** This is an example of output from the **show mac address-table move update** command:

```
Switch# show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
switch#
```

Related Commands	Command	Description
	<a href="#">clear mac address-table move update</a>	Clears the MAC address-table move update counters.
	<a href="#">mac address-table move update {receive   transmit}</a>	Configures MAC address-table move update on the switch.

---

 show mac address-table notification
 

---

## show mac address-table notification

Use the **show mac address-table notification** command in EXEC mode to display the MAC address notification settings for all interfaces or the specified interface.

**show mac address-table notification {change [interface [interface-id]] | mac-move | threshold}**

Syntax Description	change	Display the MAC change notification feature parameters and the history table.
Command Modes	interface	(Optional) Display information for all interfaces. Valid interfaces include physical ports and port channels.
Release	interface-id	(Optional) Display information for the specified interface. Valid interfaces include physical ports and port channels.
mac-move	mac-move	Display status for MAC address move notifications.
threshold	threshold	Display status for MAC-address table threshold monitoring.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.2(40)SE	The <b>change</b> , <b>mac-move</b> , and <b>threshold</b> keywords were added.

Usage Guidelines	Use the <b>show mac address-table notification change</b> command without keywords to see if the MAC address change notification feature is enabled or disabled, the MAC notification interval, the maximum number of entries allowed in the history table, and the history table contents.  Use the <b>interface</b> keyword to display the notifications for all interfaces. If the <i>interface-id</i> is included, only the flags for that interface appear.
------------------	--

**Examples**

This is an example of output from the **show mac address-table notification change** command:

```

Switch# show mac address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
-----
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added Vlan: 2      MAC Addr: 0000.0000.0001 Module: 0 Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added Vlan: 2      MAC Addr: 0000.0000.0000 Module: 0 Port: 1
Operation: Added Vlan: 2      MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Added Vlan: 2      MAC Addr: 0000.0000.0003 Module: 0 Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0 Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0 Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0 Port: 1

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>clear mac address-table notification</b></a>	Clears the MAC address notification global counters.
<a href="#"><b>mac address-table notification</b></a>	Enables the MAC address notification feature for MAC address changes, moves, or address-table thresholds.
<a href="#"><b>show mac address-table address</b></a>	Displays MAC address table information for the specified MAC address.
<a href="#"><b>show mac address-table aging-time</b></a>	Displays the aging time in all VLANs or the specified VLAN.
<a href="#"><b>show mac address-table count</b></a>	Displays the number of addresses present in all VLANs or the specified VLAN.
<a href="#"><b>show mac address-table dynamic</b></a>	Displays dynamic MAC address table entries only.
<a href="#"><b>show mac address-table interface</b></a>	Displays the MAC address table information for the specified interface.
<a href="#"><b>show mac address-table static</b></a>	Displays static MAC address table entries only.
<a href="#"><b>show mac address-table vlan</b></a>	Displays the MAC address table information for the specified VLAN.

---

 show mac address-table static
 

---

# show mac address-table static

Use the **show mac address-table static** command in EXEC mode to display only static MAC address table entries.

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

<b>Syntax Description</b>	<b>address mac-address</b> (Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
<b>interface interface-id</b>	(Optional) Specify an interface to match; valid <i>interfaces</i> include physical ports and port channels.
<b>vlan vlan-id</b>	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.

---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

---

## Command History

### Examples

This is an example of output from the **show mac address-table static** command:

```
Switch# show mac address-table static
      Mac Address Table
-----
Vlan   Mac Address      Type      Ports
----  -----
All    0100.0ccc.cccc  STATIC    CPU
All    0180.c200.0000  STATIC    CPU
All    0100.0ccc.cccd  STATIC    CPU
All    0180.c200.0001  STATIC    CPU
All    0180.c200.0004  STATIC    CPU
All    0180.c200.0005  STATIC    CPU
        4    0001.0002.0004  STATIC    Drop
        6    0001.0002.0007  STATIC    Drop
Total Mac Addresses for this criterion: 8
```

---

### Related Commands

Command	Description
<a href="#">mac address-table static</a>	Adds static addresses to the MAC address table.
<a href="#">mac address-table static drop</a>	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.

Command	Description
<b>show mac address-table interface</b>	Displays the MAC address table information for the specified interface.
<b>show mac address-table notification</b>	Displays the MAC address notification settings for all interfaces or the specified interface.
<b>show mac address-table vlan</b>	Displays the MAC address table information for the specified VLAN.

---

 show mac address-table vlan
 

---

# show mac address-table vlan

Use the **show mac address-table vlan** command in EXEC mode to display the MAC address table information for the specified VLAN.

**show mac address-table vlan *vlan-id***

<b>Syntax Description</b>	<i>vlan-id</i> (Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

This is an example of output from the **show mac address-table vlan 1** command:

```
Switch# show mac address-table vlan 1
  Mac Address Table
  -----
  Vlan      Mac Address        Type      Ports
  ----      -----            ----      -----
  1        0100.0ccc.cccc    STATIC    CPU
  1        0180.c200.0000    STATIC    CPU
  1        0100.0ccc.cccd    STATIC    CPU
  1        0180.c200.0001    STATIC    CPU
  1        0180.c200.0002    STATIC    CPU
  1        0180.c200.0003    STATIC    CPU
  1        0180.c200.0005    STATIC    CPU
  1        0180.c200.0006    STATIC    CPU
  1        0180.c200.0007    STATIC    CPU
Total Mac Addresses for this criterion: 9
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show mac address-table address</a>	Displays MAC address table information for the specified MAC address.
	<a href="#">show mac address-table aging-time</a>	Displays the aging time in all VLANs or the specified VLAN.
	<a href="#">show mac address-table count</a>	Displays the number of addresses present in all VLANs or the specified VLAN.
	<a href="#">show mac address-table dynamic</a>	Displays dynamic MAC address table entries only.
	<a href="#">show mac address-table interface</a>	Displays the MAC address table information for the specified interface.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or the specified interface.
	<a href="#">show mac address-table static</a>	Displays static MAC address table entries only.

# show mls qos

Use the **show mls qos** command in EXEC mode to display global quality of service (QoS) configuration information.

**show mls qos**

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Examples** This is an example of output from the **show mls qos** command when QoS is enabled and DSCP transparency is enabled:

```
Switch# show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Related Commands	Command	Description
	<a href="#">mls qos</a>	Enables QoS for the entire switch.

---

■ show mls qos aggregate-policer

## show mls qos aggregate-policer

Use the **show mls qos aggregate-policer** command in EXEC mode to display the quality of service (QoS) aggregate policer configuration.

**show mls qos aggregate-policer [aggregate-policer-name]**

---

<b>Syntax Description</b>	<i>aggregate-policer-name</i> (Optional) Display the policer configuration for the specified name.
---------------------------	--

---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

---

### Command History

**Usage Guidelines** A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded.

---

**Examples** This is an example of output from the **show mls qos aggregate-policer** command:

```
Switch# show mls qos aggregate-policer policer1
aggregate-policer policer1 1000000 2000000 exceed-action drop
Not used by any policy map
```

---

Related Commands	Command	Description
	<a href="#">mls qos aggregate-policer</a>	Defines policer parameters that can be shared by multiple classes within a policy map.

---

# show mls qos input-queue

Use the **show mls qos input-queue** command in EXEC mode to display quality of service (QoS) settings for the ingress queues.

**show mls qos input-queue**

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

**Examples** This is an example of output from the **show mls qos input-queue** command:

```
Switch# show mls qos input-queue
Queue : 1 2
-----
buffers : 90 10
bandwidth : 4 4
priority : 0 10
threshold1: 100 100
threshold2: 100 100
```

## Related Commands

Command	Description
<a href="#">mls qos srr-queue input bandwidth</a>	Assigns shaped round robin (SRR) weights to an ingress queue.
<a href="#">mls qos srr-queue input buffers</a>	Allocates the buffers between the ingress queues.
<a href="#">mls qos srr-queue input cos-map</a>	Maps assigned class of service (CoS) values to an ingress queue and assigns CoS values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue input dscp-map</a>	Maps assigned Differentiated Services Code Point (DSCP) values to an ingress queue and assigns DSCP values to a queue and to a threshold ID.
<a href="#">mls qos srr-queue input priority-queue</a>	Configures the ingress priority queue and guarantees bandwidth.
<a href="#">mls qos srr-queue input threshold</a>	Assigns weighted tail-drop (WTD) threshold percentages to an ingress queue.

---

 show mls qos interface
 

---

# show mls qos interface

Use the **show mls qos interface** command in EXEC mode to display quality of service (QoS) information at the port level.

**show mls qos interface [interface-id] [buffers | queueing | statistics]**

Syntax Description	<b>interface-id</b> (Optional) Display QoS information for the specified port. Valid interfaces include physical ports.
<b>buffers</b>	(Optional) Display the buffer allocation among the queues.
<b>queueing</b>	(Optional) Display the queueing strategy (shared or shaped) and the weights corresponding to the queues.
<b>statistics</b>	(Optional) Display statistics for sent and received Differentiated Services Code Points (DSCPs) and class of service (CoS) values, the number of packets enqueued or dropped per egress queue, and the number of in-profile and out-of-profile packets for each policer.

---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

---

## Command History

Though visible in the command-line help string, the **policer** keyword is not supported.

---

**Examples** This is an example of output from the **show mls qos interface interface-id buffers** command:

```
Switch# show mls qos interface gigabitethernet0/2 buffers
GigabitEthernet0/2
The port is mapped to qset : 1
The allocations between the queues are : 25 25 25 25
```

This is an example of output from the **show mls qos interface interface-id queueing** command. The egress expedite queue overrides the configured shaped round robin (SRR) weights.

```
Switch# show mls qos interface gigabitethernet0/2 queueing
GigabitEthernet0/2
Egress Priority Queue :enabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational Bandwidth:100.0)
The port is mapped to qset : 1
```

This is an example of output from the **show mls qos interface interface-id statistics** command. [Table 2-40](#) describes the fields in this display.

```
Switch# show mls qos interface gigabitethernet0/2 statistics
GigabitEthernet0/2
dscp: incoming
-----
```

```

      0 - 4 :      4213      0      0      0      0
      5 - 9 :        0      0      0      0      0
     10 - 14 :       0      0      0      0      0
     15 - 19 :       0      0      0      0      0
     20 - 24 :       0      0      0      0      0
     25 - 29 :       0      0      0      0      0
     30 - 34 :       0      0      0      0      0
     35 - 39 :       0      0      0      0      0
     40 - 44 :       0      0      0      0      0
     45 - 49 :       0      0      0      6      0
     50 - 54 :       0      0      0      0      0
     55 - 59 :       0      0      0      0      0
     60 - 64 :       0      0      0      0      0
      dscp: outgoing
-----
      0 - 4 :    363949      0      0      0      0
      5 - 9 :        0      0      0      0      0
     10 - 14 :       0      0      0      0      0
     15 - 19 :       0      0      0      0      0
     20 - 24 :       0      0      0      0      0
     25 - 29 :       0      0      0      0      0
     30 - 34 :       0      0      0      0      0
     35 - 39 :       0      0      0      0      0
     40 - 44 :       0      0      0      0      0
     45 - 49 :       0      0      0      0      0
     50 - 54 :       0      0      0      0      0
     55 - 59 :       0      0      0      0      0
     60 - 64 :       0      0      0      0      0
      cos: incoming
-----
      0 - 4 :    132067      0      0      0      0
      5 - 9 :        0      0      0      0      0
      cos: outgoing
-----
      0 - 4 :    739155      0      0      0      0
      5 - 9 :        90      0      0      0      0
      Policer: Inprofile:      0 OutofProfile:      0

```

**Table 0-14** show mls qos interface statistics Field Descriptions

Field		Description
DSCP	incoming	Number of packets received for each DSCP value.
	outgoing	Number of packets sent for each DSCP value.
CoS	incoming	Number of packets received for each CoS value.
	outgoing	Number of packets sent for each CoS value.
Policer	Inprofile	Number of in profile packets for each policer.
	Outofprofile	Number of out-of-profile packets for each policer.

**Related Commands**

show mls qos interface

Command	Description
<b>mls qos queue-set output buffers</b>	Allocates buffers to a queue-set.
<b>mls qos queue-set output threshold</b>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
<b>mls qos srr-queue input bandwidth</b>	Assigns SRR weights to an ingress queue.
<b>mls qos srr-queue input buffers</b>	Allocates the buffers between the ingress queues.
<b>mls qos srr-queue input cos-map</b>	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue input dscp-map</b>	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
<b>mls qos srr-queue input priority-queue</b>	Configures the ingress priority queue and guarantees bandwidth.
<b>mls qos srr-queue input threshold</b>	Assigns WTD threshold percentages to an ingress queue.
<b>mls qos srr-queue output cos-map</b>	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
<b>mls qos srr-queue output dscp-map</b>	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.
<b>policy-map</b>	Creates or modifies a policy map.
<b>priority-queue</b>	Enables the egress expedite queue on a port.
<b>queue-set</b>	Maps a port to a queue-set.
<b>srr-queue bandwidth limit</b>	Limits the maximum output on a port.
<b>srr-queue bandwidth shape</b>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
<b>srr-queue bandwidth share</b>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

# show mls qos maps

Use the **show mls qos maps** command in EXEC mode to display quality of service (QoS) mapping information.

```
show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q |
dscp-mutation dscp-mutation-name | dscp-output-q | ip-prec-dscp | policed-dscp]
```

Syntax Description	
<b>cos-dscp</b>	(Optional) Display class of service (CoS)-to-DSCP map.
<b>cos-input-q</b>	(Optional) Display the CoS input queue threshold map.
<b>cos-output-q</b>	(Optional) Display the CoS output queue threshold map.
<b>dscp-cos</b>	(Optional) Display DSCP-to-CoS map.
<b>dscp-input-q</b>	(Optional) Display the DSCP input queue threshold map.
<b>dscp-mutation <i>dscp-mutation-name</i></b>	(Optional) Display the specified DSCP-to-DSCP-mutation map.
<b>dscp-output-q</b>	(Optional) Display the DSCP output queue threshold map.
<b>ip-prec-dscp</b>	(Optional) Display the IP-precedence-to-DSCP map.
<b>policed-dscp</b>	(Optional) Display the policed-DSCP map.

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

**Usage Guidelines** During classification, QoS uses the mapping tables to represent the priority of the traffic and to derive a corresponding class of service (CoS) or Differentiated Services Code Point (DSCP) value from the received CoS, DSCP, or IP precedence value.

The policed-DSCP, DSCP-to-CoS, and the DSCP-to-DSCP-mutation maps appear as a matrix. The d1 column specifies the most-significant digit in the DSCP. The d2 row specifies the least-significant digit in the DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, a DSCP value of 43 corresponds to a CoS value of 5.

The DSCP input queue threshold and the DSCP output queue threshold maps appear as a matrix. The d1 column specifies the most-significant digit of the DSCP number. The d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID. For example, in the DSCP input queue threshold map, a DSCP value of 43 corresponds to queue 2 and threshold 1 (02-01).

The CoS input queue threshold and the CoS output queue threshold maps show the CoS value in the top row and the corresponding queue ID and threshold ID in the second row. For example, in the CoS input queue threshold map, a CoS value of 5 corresponds to queue 2 and threshold 1 (2-1).

## Examples

This is an example of output from the **show mls qos maps** command:

```
Switch# show mls qos maps
```

show mls qos maps

```

Policed-dscp map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63

Dscp-cos map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 01 01
1 : 01 01 01 01 01 01 02 02 02 02
2 : 02 02 02 03 03 03 03 03 03 03
3 : 03 03 04 04 04 04 04 04 04 04
4 : 05 05 05 05 05 05 05 05 06 06
5 : 06 06 06 06 06 06 07 07 07 07
6 : 07 07 07 07 07 07 07 07 07 07

Cos-dscp map:
cos: 0 1 2 3 4 5 6 7
-----
dscp: 0 8 16 24 32 40 48 56

IpPrecedence-dscp map:
ipprec: 0 1 2 3 4 5 6 7
-----
dscp: 0 8 16 24 32 40 48 56

Dscp-outputq-threshold map:
d1 :d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01
1 : 02-01 02-01 02-01 02-01 02-01 02-01 03-01 03-01 03-01 03-01 03-01
2 : 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01 03-01
3 : 03-01 03-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
4 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 04-01 04-01
5 : 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01
6 : 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01 04-01

Dscp-inputq-threshold map:
d1 :d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
1 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
2 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
3 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
4 : 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 02-01 01-01 01-01
5 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
6 : 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01

Cos-outputq-threshold map:
cos: 0 1 2 3 4 5 6 7
-----
queue-threshold: 2-1 2-1 3-1 3-1 4-1 1-1 4-1 4-1

Cos-inputq-threshold map:
cos: 0 1 2 3 4 5 6 7
-----
queue-threshold: 1-1 1-1 1-1 1-1 1-1 2-1 1-1 1-1

```

```
Dscp-dscp mutation map:
Default DSCP Mutation Map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```

Related Commands	Command	Description
	<a href="#">mls qos map</a>	Defines the CoS-to-DSCP map, DSCP-to-CoS map, DSCP-to-DSCP-mutation map, IP-precedence-to-DSCP map, and the policed-DSCP map.
	<a href="#">mls qos srr-queue input cos-map</a>	Maps CoS values to an ingress queue or maps CoS values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue input dscp-map</a>	Maps DSCP values to an ingress queue or maps DSCP values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue output cos-map</a>	Maps CoS values to an egress queue or maps CoS values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue output dscp-map</a>	Maps DSCP values to an egress queue or maps DSCP values to a queue and to a threshold ID.

---

■ show mls qos queue-set

## show mls qos queue-set

Use the **show mls qos queue-set** command in EXEC mode to display quality of service (QoS) settings for the egress queues.

**show mls qos queue-set [qset-id]**

<b>Syntax Description</b>	<i>qset-id</i> (Optional) ID of the queue-set. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port. The range is 1 to 2.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

### Command History

#### Examples

This is an example of output from the **show mls qos queue-set** command:

```
Switch# show mls qos queue-set
QueueSet: 1
Queue : 1 2 3 4
-----
buffers : 25 25 25 25
threshold1: 100 200 100 100
threshold2: 100 200 100 100
reserved : 50 50 50 50
maximum : 400 400 400 400
QueueSet: 2
Queue : 1 2 3 4
-----
buffers : 25 25 25 25
threshold1: 100 200 100 100
threshold2: 100 200 100 100
reserved : 50 50 50 50
maximum : 400 400 400 400
```

Related Commands	Command	Description
	<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to the queue-set.
	<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation of the queue-set.

# show mls qos vlan

Use the **show mls qos vlan** command in EXEC mode to display the policy maps attached to a switch virtual interface (SVI).

**show mls qos vlan *vlan-id***

<b>Syntax Description</b>	<i>vlan-id</i>	Specify the VLAN ID of the SVI to display the policy maps. The range is 1 to 4094.
---------------------------	----------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

**Usage Guidelines** The output from the **show mls qos vlan** command is meaningful only when VLAN-based quality of service (QoS) is enabled and when policy maps are configured.

**Examples** This is an example of output from the **show mls qos vlan** command:

```
Switch# show mls qos vlan 10
Vlan10
Attached policy-map for Ingress:pm-test-pm-2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports and enters policy-map configuration mode.

**show monitor**

# show monitor

Use the **show monitor** command in EXEC mode to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch.

**show monitor [session {session\_number | all | local | range list | remote}]**

## Syntax Description

<b>session</b>	(Optional) Display information about specified SPAN sessions.
<b>session_number</b>	Specify the number of the SPAN or RSPAN session. The range is 1 to 66.
<b>all</b>	Display all SPAN sessions.
<b>local</b>	Display only local SPAN sessions.
<b>range list</b>	Display a range of SPAN sessions, where <i>list</i> is the range of valid sessions, 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>	Display only remote SPAN sessions.
<b>detail</b>	(Optional) Display detailed information about the specified sessions.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

### Usage Guidelines

Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

The output is the same for the **show monitor** command and the **show monitor session all** command.

## Examples

This is an example of output for the **show monitor** command:

```
Switch# show monitor
Session 1
-----
Type : Local Session
Source Ports :
Encapsulation : Replicate
Ingress : Disabled

Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

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

```
Switch# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
Encapsulation : Replicate
Ingress : Disabled
```

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

```
Switch# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q

Session 2
-----
Type : Local Session
Source Ports :
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

#### Related Commands

Command	Description
<a href="#">monitor session</a>	Starts or modifies a SPAN or RSPAN session.

**show mvr**

## show mvr

Use the **show mvr** privileged EXEC command without keywords to display the current Multicast VLAN Registration (MVR) global parameter values.

**show mvr**

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

**Command Modes** Privileged EXEC

### Command History

#### Usage Guidelines

The command information includes whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible).

### Examples

This is an example of output from the **show mvr** command. The maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

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

### Related Commands

Command	Description
<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
<a href="#">mvr (interface configuration)</a>	Configures MVR ports.
<a href="#">show mvr interface</a>	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the <b>interface</b> and <b>members</b> keywords are appended to the command.
<a href="#">show mvr members</a>	Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive.

# show mvr interface

Use the **show mvr interface** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) receiver and source ports.

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

<b>Syntax Description</b>	<p><b>interface-id</b> (Optional) Display MVR type, status, and Immediate Leave setting for the interface.</p> <p><b>Note</b> Valid interfaces include physical ports (including type, module, and port number).</p>
<b>members</b>	(Optional) Display all MVR groups to which the specified interface belongs.
<b>vlan vlan-id</b>	(Optional) Display all MVR group members on this VLAN. The range is 1 to 4094.

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

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

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

Use the command with keywords to display MVR parameters for a specific receiver port.

## Examples

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

```
Switch# show mvr interface
Port      Type          Status        Immediate Leave
----      ----          -----        -----

```

In the preceding display, Status is defined as follows:

- Active means the port is part of a VLAN.
- Up/Down means that the port is forwarding/nonforwarding.
- Inactive means that the port is not yet part of any VLAN.

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

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

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

```
Switch# show mvr interface gigabitethernet0/2 members
239.255.0.0    DYNAMIC ACTIVE
239.255.0.1    DYNAMIC ACTIVE
239.255.0.2    DYNAMIC ACTIVE
239.255.0.3    DYNAMIC ACTIVE
```

■ **show mvr interface**

```
239.255.0.4      DYNAMIC ACTIVE
239.255.0.5      DYNAMIC ACTIVE
239.255.0.6      DYNAMIC ACTIVE
239.255.0.7      DYNAMIC ACTIVE
239.255.0.8      DYNAMIC ACTIVE
239.255.0.9      DYNAMIC ACTIVE
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>mvr (global configuration)</b></a>	Enables and configures multicast VLAN registration on the switch.
	<a href="#"><b>mvr (interface configuration)</b></a>	Configures MVR ports.
	<a href="#"><b>show mvr</b></a>	Displays the global MVR configuration on the switch.
	<a href="#"><b>show mvr members</b></a>	Displays all receiver ports that are members of an MVR multicast group.

# show mvr members

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

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

<b>Syntax Description</b>	<i>ip-address</i>	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.
---------------------------	-------------------	---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

<b>Usage Guidelines</b>	The <b>show mvr members</b> command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.
-------------------------	--

<b>Examples</b>	This is an example of output from the <b>show mvr members</b> command:
-----------------	--

```
Switch# show mvr members
MVR Group IP      Status        Members
-----  -----
239.255.0.2      INACTIVE     None
239.255.0.3      INACTIVE     None
239.255.0.4      INACTIVE     None
239.255.0.5      INACTIVE     None
239.255.0.6      INACTIVE     None
239.255.0.7      INACTIVE     None
239.255.0.8      INACTIVE     None
239.255.0.9      INACTIVE     None
239.255.0.10     INACTIVE     None

<output truncated>
```

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

```
Switch# show mvr members 239.255.0.2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">mvr (global configuration)</a>	Enables and configures multicast VLAN registration on the switch.
	<a href="#">mvr (interface configuration)</a>	Configures MVR ports.

**show mvr members**

Command	Description
<b>show mvr</b>	Displays the global MVR configuration on the switch.
<b>show mvr interface</b>	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the <b>members</b> keyword is appended to the command.

# show network-policy profile

Use the **show network policy profile** privileged EXEC command to display the network-policy profiles.

**show network-policy profile [profile number] [detail]**

<b>Syntax Description</b>	<p><b>profile number</b> (Optional) Display the network-policy profile number. If no profile is entered, all network-policy profiles appear.</p> <p><b>detail</b> (Optional) Display detailed status and statistics information.</p>
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show network-policy profile</b> command:
	<pre>Switch# show network-policy profile Network Policy Profile 10   voice vlan 17 cos 4   Interface:     none Network Policy Profile 30   voice vlan 30 cos 5   Interface:     none Network Policy Profile 36   voice vlan 4 cos 3   Interface:     Interface_id</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">network-policy</a>	Applies a network-policy to an interface.
	<a href="#">network-policy profile (global configuration)</a>	Creates the network-policy profile.
	<a href="#">network-policy profile (network-policy configuration)</a>	Configures the attributes of network-policy profiles.

**show nmsp**

## show nmsp

Use the **show nmsp** privileged EXEC command to display the Network Mobility Services Protocol (NMSP) information for the switch. This command is available only when your switch is running the cryptographic (encrypted) software image.

```
show nmsp {attachment suppress interface | capability | notification interval | statistics
{connection | summary} | status | subscription {detail | summary}}
```

<b>Syntax Description</b>	
<b>attachment suppress interface</b>	Display attachment suppress interfaces.
<b>capability</b>	Display switch capabilities including the supported services and subservices.
<b>notification interval</b>	Display the notification intervals of the supported services.
<b>statistics {connection   summary}</b>	Display the NMSP statistics information. <ul style="list-style-type: none"> <li>• <b>connection</b>—display the message counters on each connection.</li> <li>• <b>summary</b>—display the global counters.</li> </ul>
<b>status</b>	Display information about the NMSP connections.
<b>subscription {detail   summary}</b>	Display the subscription information on each NMSP connection. <ul style="list-style-type: none"> <li>• <b>detail</b>—display all services and subservices subscribed on each connection.</li> <li>• <b>summary</b>—display all services subscribed on each connection.</li> </ul>

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show nmsp attachment suppress interface</b> command:
	<pre>Switch# show nmsp attachment suppress interface NMSP Attachment Suppression Interfaces ----- GigabitEthernet1/1 GigabitEthernet1/2</pre>

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

```
Switch# show nmsp capability
NMSP Switch Capability
-----
Service      Subservice
-----
Attachment   Wired Station
Location     Subscription
```

This is an example of output from the **show nmsp notification interval** command:

```
Switch# show nmsp notification interval
NMSP Notification Intervals
-----
Attachment notify interval: 30 sec (default)
Location notify interval: 30 sec (default)
```

This is an example of output from the **show nmsp statistics connection** and **show nmsp statistics summary** commands:

```
Switch# show nmsp statistics connection
NMSP Connection Counters
-----
Connection 1:
    Connection status: UP
    Freed connection: 0

    Tx message count      Rx message count
    -----                  -----
    Subscr Resp: 1          Subscr Req: 1
    Capa Notif: 1           Capa Notif: 1
    Atta Resp: 1            Atta Req: 1
    Atta Notif: 0
    Loc Resp: 1             Loc Req: 1
    Loc Notif: 0
    Unsupported msg: 0

Switch# show nmsp statistics summary
NMSP Global Counters
-----
    Send too big msg: 0
    Failed socket write: 0
    Partial socket write: 0
    Socket write would block: 0
    Failed socket read: 0
    Socket read would block: 0
    Transmit Q full: 0
    Max Location Notify Msg: 0
    Max Attachment Notify Msg: 0
    Max Tx Q Size: 0
```

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

```
Switch# show nmsp status
NMSP Status
-----
NMSP: enabled
MSE IP Address      TxEchoResp RxEchoReq TxData RxData
172.19.35.109       5      5     4     4
```

This is an example of output from the **show nmsp show subscription detail** and the **show nmsp show subscription summary** commands:

```
Switch# show nmsp subscription detail
Mobility Services Subscribed by 172.19.35.109:
Services          Subservices
-----
Attachment:      Wired Station
Location:        Subscription

Switch# show nmsp subscription summary
Mobility Services Subscribed:
MSE IP Address   Services
```

**show nmsp**-----  
172.19.35.109      Attachment, Location**Related Commands**

Command	Description
<a href="#">clear nmsp statistics</a>	Clears the NMSP statistic counters.
<a href="#">nmsp</a>	Enables Network Mobility Services Protocol (NMSP) on the switch.

# show pagp

Use the **show pagp** command in EXEC mode to display Port Aggregation Protocol (PAgP) channel-group information.

```
show pagp [channel-group-number] {counters | dual-active | internal | neighbor} ]
```

## Syntax Description

<i>channel-group-number</i>	(Optional) Number of the channel group. The range is 1 to .
<b>counters</b>	Display traffic information.
<b>dual-active</b>	Display the dual-active status.
<b>internal</b>	Display internal information.
<b>neighbor</b>	Display neighbor information.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.2(46)SE	The <b>dual-active</b> keyword was added.

## Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

## Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch# show pagp 1 counters
          Information           Flush
Port      Sent    Recv      Sent    Recv
-----
Channel group: 1
```

**show pagp**

This is an example of output from the **show pagp 1 internal** command:

```
Switch# show pagp 1 internal
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.
Timers: H - Hello timer is running.          Q - Quit timer is running.
       S - Switching timer is running.        I - Interface timer is running.

Channel group 1
      Hello    Partner   PAgP     Learning   Group
Port      Flags State Timers Interval Count Priority Method Ifindex
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch# show pagp 1 neighbor
Flags: S - Device is sending Slow hello. C - Device is in Consistent state.
       A - Device is in Auto mode.          P - Device learns on physical port.

Channel group 1 neighbors
      Partner      Partner      Partner      Partner Group
Port      Name       Device ID     Port       Age   Flags   Cap.
```

This is an example of output from the **show pagp dual-active** command:

```
Switch# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
      Dual-Active    Partner      Partner      Partner
Port      Detect Capable  Name       Port       Version

<output truncated>
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">clear pagp</a>	Clears PAgP channel-group information.

# show policy-map

Use the **show policy-map** command in EXEC mode to display quality of service (QoS) policy maps, which define classification criteria for incoming traffic.

**show policy-map [policy-map-name [class class-map-name]]**

<b>Syntax Description</b>	<i>policy-map-name</i> (Optional) Display the specified policy-map name. <i>class class-map-name</i> (Optional) Display QoS policy actions for a individual class.
---------------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

Though visible in the command-line help string, the **control-plane** and **interface** keywords are not supported, and the statistics shown in the display should be ignored.

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

## Examples

This is an example of output from the **show policy-map** command:

```
Switch# show policy-map
Policy Map videowizard_policy2
  class videowizard_10-10-10-10
    set dscp 34
    police 100000000 2000000 exceed-action drop

  Policy Map mypolicy
    class dscp5
      set dscp 6
```

Related Commands	Command	Description
	<a href="#">policy-map</a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

**show port-security**

# show port-security

Use the **show port-security** privileged EXEC command to display port-security settings for an interface or for the switch.

**show port-security [interface *interface-id*] [address | vlan]**

<b>Syntax Description</b>	<b>interface <i>interface-id</i></b>	<b>Note</b>	(Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number).
	<b>address</b>		(Optional) Display all secure MAC addresses on all ports or a specified port.
	<b>vlan</b>		(Optional) Display port security settings for all VLANs on the specified interface. This keyword is visible only on interfaces that have the switchport mode set to <b>trunk</b> .

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

If you enter the command without keywords, the output includes the administrative and operational status of all secure ports on the switch.

If you enter an *interface-id*, the command displays port security settings for the interface.

If you enter the **address** keyword, the command displays the secure MAC addresses for all interfaces and the aging information for each secure address.

If you enter an *interface-id* and the **address** keyword, the command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

If you enter the **vlan** keyword, the command displays the configured maximum and the current number of secure MAC addresses for all VLANs on the interface. This option is visible only on interfaces that have the switchport mode set to **trunk**.

### Examples

This is an example of the output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                  (Count)        (Count)       (Count)
-----
Gi0/1           1              0              0                Shutdown
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface *interface-id*** command:

```
Switch# show port-security interface gigabitethernet0/1
Port Security : Enabled
Port status   : SecureUp
Violation mode : Shutdown
```

```
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

This is an example of output from the **show port-security address** command:

```
Switch# show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type          Ports      Remaining Age
                                         (mins)
-----
---  -----
  1    0006.0700.0800  SecureConfigured  Gi0/2      1
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface gigabitethernet0/2 address** command:

```
Switch# show port-security interface gigabitethernet0/2 address
Secure Mac Address Table
-----
Vlan    Mac Address      Type          Ports      Remaining Age
                                         (mins)
-----
---  -----
  1    0006.0700.0800  SecureConfigured  Gi0/2      1
-----
Total Addresses: 1
```

This is an example of output from the **show port-security interface *interface-id* vlan** command:

```
Switch# show port-security interface gigabitethernet0/2 vlan
Default maximum:not set, using 5120
VLAN  Maximum   Current
      5       default     1
      10      default    54
      11      default   101
      12      default   101
      13      default  201
      14      default  501
```

Related Commands	Command	Description
	<a href="#">clear port-security</a>	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
	<a href="#">switchport port-security</a>	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

**show power inline**

# show power inline

Use the **show power inline** command in EXEC mode to display the Power over Ethernet (PoE) status for the specified PoE port or for all PoE ports.

**show power inline [interface-id | consumption]**

<b>Syntax Description</b>	<i>interface-id</i> (Optional) Display PoE-related power management information for the specified interface. <b>consumption</b> (Optional) Display the power allocated to devices connected to PoE ports.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Examples

This is an example of output from the **show power inline** command . In the display, port 2 is configured as static; power has been pre-allocated to this port, but no powered device is connected. Port 6 is a static port in the power-deny state because its maximum wattage is configured for 10 W. The connected powered device has a reported class maximum wattage for a Class 0 or Class 3 device. [Table 2-41](#) describes the output fields.

**Table 0-15 show power inline Field Descriptions**

Field	Description
Admin	Administration mode: auto, off, static
Oper	Operating mode: <ul style="list-style-type: none"> <li>• on—the powered device is detected, and power is applied.</li> <li>• off—no PoE is applied.</li> <li>• faulty—device detection or a powered device is in a faulty state.</li> <li>• power-deny—a powered device is detected, but no PoE is available, or the maximum wattage exceeds the detected powered-device maximum.</li> </ul>
Power	The supplied PoE in watts
Device	The device type detected: n/a, unknown, Cisco powered-device, IEEE powered-device, <name from CDP>
Class	The IEEE classification: n/a, Class <0–4>
Available	The total amount of PoE in the system
Used	The amount of PoE allocated to ports
Remaining	The amount of PoE not allocated to ports in the system. (Available – Used = Remaining)

This is an example of output from the **show power inline** command on a port:

This is an example of output from the **show power inline consumption** command on all PoE switch ports:

```
Switch# show power inline consumption
Default PD consumption : 15400 mW
```

Related Commands	Command	Description
	<a href="#">logging event</a>	Enables the logging of PoE events.
	<a href="#">power-inline-status</a>	
	<a href="#">power inline</a>	Configures the power management mode for the specified PoE port or for all PoE ports.
	<a href="#">show controllers</a>	Displays the values in the registers of the specified PoE controller.
	<a href="#">power inline</a>	

**show psp config**

## show psp config

To display the status of protocol storm protection configured for a specific protocol on a VLAN, use the **show psp config** privileged EXEC command.

```
show psp config {arp | dhcp | igmp}
```

### Syntax Description

<b>arp</b>	Show protocol storm protection status for ARP and ARP snooping.
<b>dhcp</b>	Show protocol storm protection status for DHCP and DHCP snooping.
<b>igmp</b>	Show protocol storm protection status for IGMP and IGMP snooping.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.2(58)SE	This command was introduced.

### Examples

This is an example of output from the **show psp config dhcp** command with protocol storm protection configured to drop packets when the incoming rate exceeds 35 packets per second.

```
Switch# show psp config dhcp
-----
PSP Protocol Configuration Summary:
-----
DHCP Rate Limit      : 35 packets/sec
PSP Action           : Packet Drop
```

### Related Commands

Command	Description
<b>psp {arp   dhcp   igmp} pps value</b>	Configures protocol storm protection for ARP, DHCP, or IGMP.
<b>show psp statistics</b>	Displays the number of dropped packets when protocol storm protection is configured.
<b>clear psp counter</b>	Clears the counter of dropped packets.

# show psp statistics

To display the number of packets dropped for all protocols when protocol storm protection is configured, use the **show psp statistics** privileged EXEC command.

**show psp statistics [arp | dhcp | igmp]**

<b>Syntax Description</b>	<b>arp</b> (Optional) Show the number of packets dropped for ARP and ARP snooping. <b>dhcp</b> (Optional) Show the number of packets dropped for DHCP and DHCP snooping. <b>igmp</b> (Optional) Show the number of packets dropped for IGMP and IGMP snooping.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(58)SE	This command was introduced.

<b>Examples</b>	This is an example of output from the <b>show psp statistics dhcp</b> command when protocol storm protection is configured for DHCP. The output shows that 13 packets were dropped.
-----------------	---

```
Switch# show psp statistics dhcp
-----
PSP Protocol Drop Counter Summary:
-----
DHCP Drop Counter: 13
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>psp {arp   dhcp   igmp} pps value</b>	Configures protocol storm protection for ARP, DHCP, or IGMP.
	<b>show psp config</b>	Displays the protocol storm protection configuration.
	<b>clear psp counter</b>	Clears the counter of dropped packets.

**show setup express**

# show setup express

Use the **show setup express** privileged EXEC command to display if Express Setup mode is active on the switch.

**show setup express**

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

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

## Command History

**Examples** This is an example of output from the **show setup express** command:

```
Switch# show setup express
express setup mode is active
```

## Related Commands

Command	Description
<a href="#">setup express</a>	Enables Express Setup mode.

# show spanning-tree

Use the **show spanning-tree** command in EXEC mode to display spanning-tree state information.

```
show spanning-tree [bridge-group | active [detail] | backbonefast | blockedports | bridge | detail [active] | inconsistentports | interface interface-id | mst | pathcost method | root | summary [totals] | uplinkfast | vlan vlan-id]

show spanning-tree bridge-group [active [detail] | blockedports | bridge | detail [active] | inconsistentports | interface interface-id | root | summary]

show spanning-tree vlan vlan-id [active [detail] | blockedports | bridge | detail [active] | inconsistentports | interface interface-id | root | summary]

show spanning-tree {vlan vlan-id | bridge-group} bridge [address | detail | forward-time | hello-time | id | max-age | priority [system-id] | protocol]

show spanning-tree {vlan vlan-id | bridge-group} root [address | cost | detail | forward-time | hello-time | id | max-age | port | priority [system-id]

show spanning-tree interface interface-id [active [detail] | cost | detail [active] | inconsistency | portfast | priority | rootcost | state]

show spanning-tree mst [configuration [digest]] | [instance-id [detail | interface interface-id [detail]]]
```

Syntax Description	
<b>bridge-group</b>	(Optional) Specify the bridge group number. The range is 1 to 255.
<b>active [detail]</b>	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
<b>backbonefast</b>	(Optional) Display spanning-tree BackboneFast status.
<b>blockedports</b>	(Optional) Display blocked port information (available only in privileged EXEC mode).
<b>bridge [address   detail   forward-time   hello-time   id   max-age   priority [system-id]   protocol]</b>	(Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode).
<b>detail [active]</b>	(Optional) Display a detailed summary of interface information ( <b>active</b> keyword available only in privileged EXEC mode).
<b>inconsistentports</b>	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
<b>interface interface-id [active [detail]   cost   detail [active]   inconsistency   portfast   priority   rootcost   state]</b>	(Optional) Display spanning-tree information for the specified interface (all options except <b>portfast</b> and <b>state</b> available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to .

---

```
show spanning-tree
```

---

<b>mst [configuration [digest]] [instance-id [detail   interface interface-id [detail]]]</b>	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode).  The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>digest</b>—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode).</li></ul> The terminology was updated for the implementation of the IEEE standard, and the <i>txholdcount</i> field was added. The new master role appears for boundary ports. The word <i>pre-standard</i> or <i>Pre-STD</i> appears when an IEEE standard bridge sends prestandard BPDUs on a port. The word <i>pre-standard (config)</i> or <i>Pre-STD-Cf</i> appears when a port has been configured to transmit prestandard BPDUs and no prestandard BPDU has been received on that port. The word <i>pre-standard (rcvd)</i> or <i>Pre-STD-Rx</i> appears when a prestandard BPDU has been received on a port that has not been configured to transmit prestandard BPDUs. A <i>dispute</i> flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated.
<b>pathcost method</b>	(Optional) Display the default path cost method (available only in privileged EXEC mode).
<b>root [address   cost   detail   forward-time   hello-time   id   max-age   port   priority [system-id]]</b>	(Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode).
<b>summary [totals]</b>	(Optional) Display a summary of port states or the total lines of the spanning-tree state section. The words <i>IEEE Standard</i> identify the MST version running on a switch.
<b>uplinkfast</b>	(Optional) Display spanning-tree UplinkFast status.
<b>vlan vlan-id [active [detail]   backbonefast   blockedports   bridge [address   detail   forward-time   hello-time   id   max-age   priority [system-id]   protocol]</b>	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

**Command History**

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

**Examples**

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
    Root ID  Priority    32768
              Address   0001.42e2.cdd0
              Cost       3038
              Port      24 (GigabitEthernet0/1)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID Priority    49153 (priority 49152 sys-id-ext 1)
              Address   0003.fd63.9580
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
    Uplinkfast enabled

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----  ---  -----  -----  -----
<output truncated>
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 1 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times: hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled

  Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
    Port path cost 3019, Port priority 128, Port Identifier 128.24.
    Designated root has priority 32768, address 0001.42e2.cdd0
    Designated bridge has priority 32768, address 00d0.bbf5.c680
    Designated port id is 128.25, designated path cost 19
    Timers: message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface interface-id** command:

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan      Role Sts Cost      Prio.Nbr Type
-----  -----  ---  -----  -----  -----
VLAN0001  Root FWD 3019      128.24    P2p
```

■ **show spanning-tree**

```

Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID    is enabled
Portfast                is disabled by default
PortFast BPDU Guard    is disabled by default
Portfast BPDU Filter   is disabled by default
Loopguard               is disabled by default
UplinkFast              is enabled
BackboneFast             is enabled
Pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----        -----  -----  -----  -----  -----  -----
VLAN0001      1        0        0        11       12
VLAN0002      3        0        0        1         4
VLAN0004      3        0        0        1         4
VLAN0006      3        0        0        1         4
VLAN0031      3        0        0        1         4
VLAN0032      3        0        0        1         4
<output truncated>
-----        -----  -----  -----  -----  -----
37 vlans      109      0        0        47       156
Station update rate set to 150 packets/sec.

UplinkFast statistics
-----
Number of transitions via uplinkFast (all VLANs)      : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0

BackboneFast statistics
-----
Number of transition via backboneFast (all VLANs)      : 0
Number of inferior BPDUs received (all VLANs)        : 0
Number of RLQ request PDUs received (all VLANs)      : 0
Number of RLQ response PDUs received (all VLANs)     : 0
Number of RLQ request PDUs sent (all VLANs)          : 0
Number of RLQ response PDUs sent (all VLANs)         : 0

```

This is an example of output from the **show spanning-tree mst configuration** command:

```

Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----  -----
0        1-9,21-4094
1        10-20
-----
```

This is an example of output from the **show spanning-tree mst interface interface-id** command:

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no          (default)      port guard : none      (default)
Link type: point-to-point (auto)      bpdu filter: disable  (default)
Boundary : boundary      (STP)        bpdu guard : disable  (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0       root FWD   200000     128  1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
##### MST00      vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root       address 0001.4297.e000  priority  32768 (32768 sysid 0)
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface      role state cost      prio type
-----      ----- ----- ----- -----
Port-channel1  desg FWD   200000     128  P2P bound(STP)
```

## Related Commands

Command	Description
<a href="#">clear spanning-tree counters</a>	Clears the spanning-tree counters.
<a href="#">clear spanning-tree detected-protocols</a>	Restarts the protocol migration process.
<a href="#">spanning-tree backbonefast</a>	Enables the BackboneFast feature.
<a href="#">spanning-tree bpdufilter</a>	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
<a href="#">spanning-tree bpduguard</a>	Puts an interface in the error-disabled state when it receives a BPDU.
<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
<a href="#">spanning-tree extend system-id</a>	Enables the extended system ID feature.
<a href="#">spanning-tree guard</a>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
<a href="#">spanning-tree link-type</a>	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
<a href="#">spanning-tree loopguard default</a>	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
<a href="#">spanning-tree mst configuration</a>	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
<a href="#">spanning-tree mst cost</a>	Sets the path cost for MST calculations.
<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello BPDUs sent by root switch configuration messages.
<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.

show spanning-tree

Command	Description
<b>spanning-tree mst max-hops</b>	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
<b>spanning-tree mst port-priority</b>	Configures an interface priority.
<b>spanning-tree mst priority</b>	Configures the switch priority for the specified spanning-tree instance.
<b>spanning-tree mst root</b>	Configures the MST root switch priority and timers based on the network diameter.
<b>spanning-tree port-priority</b>	Configures an interface priority.
<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface and all its associated VLANs.
<b>spanning-tree uplinkfast</b>	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
<b>spanning-tree vlan</b>	Configures spanning tree on a per-VLAN basis.

# show storm-control

Use the **show storm-control** command in EXEC mode to display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface or to display storm-control history.

**show storm-control [interface-id] [broadcast | multicast | unicast]**

Syntax Description	interface-id	Note	(Optional) Interface ID for the physical port (including type, module, and port number).
	<b>broadcast</b>	(Optional)	Display broadcast storm threshold setting.
	<b>multicast</b>	(Optional)	Display multicast storm threshold setting.
	<b>unicast</b>	(Optional)	Display unicast storm threshold setting.
	<b>  begin</b>	(Optional)	Display begins with the line that matches the <i>expression</i> .
	<b>  exclude</b>	(Optional)	Display excludes lines that match the <i>expression</i> .
	<b>  include</b>	(Optional)	Display includes lines that match the specified <i>expression</i> .
	<i>expression</i>		Expression in the output to use as a reference point.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

### Usage Guidelines

When you enter an *interface-id*, the storm control thresholds appear for the specified interface. If you do not enter an *interface-id*, settings appear for one traffic type for all ports on the switch. If you do not enter a traffic type, settings appear for broadcast storm control.

## Examples

This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch# show storm-control
Interface      Filter State    Upper       Lower       Current
-----  -----  -----  -----  -----
<output truncated>
```

**show storm-control**

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch#Switch# show storm-control gigabitethernet 0/1
Interface      Filter State    Upper       Lower      Current
-----          -----          -----       -----      -----

```

[Table 2-42](#) describes the fields in the **show storm-control** display.

**Table 0-16** *show storm-control Field Descriptions*

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: <ul style="list-style-type: none"> <li>• Blocking—Storm control is enabled, and a storm has occurred.</li> <li>• Forwarding—Storm control is enabled, and no storms have occurred.</li> <li>• Inactive—Storm control is disabled.</li> </ul>
Upper	Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Current	Displays the bandwidth usage of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled.

**Related Commands**

Command	Description
<a href="#">storm-control</a>	Sets the broadcast, multicast, or unicast storm control levels for the switch.

# show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum transmission unit (MTU) or maximum packet size set for the switch.

**show system mtu**

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

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** If you have used the **system mtu** or **system mtu jumbo** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

The system MTU refers to ports operating at 10/100 Mb/s; the system jumbo MTU refers to Gigabit ports; the system routing MTU refers to routed ports.

**Examples** This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1550 bytes
```

## Related Commands

Command	Description
<a href="#">system mtu</a>	Sets the MTU size for the Fast Ethernet, Gigabit Ethernet, or routed ports.

**show udld**

## show udld

Use the **show udld** command in EXEC mode to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

**show udld [interface-id]**

<b>Syntax Description</b>	<i>interface-id</i> (Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	
<b>Usage Guidelines</b>	If you do not enter an <i>interface-id</i> , administrative and operational UDLD status for all interfaces appear.

<b>Examples</b>	This is an example of output from the <b>show udld interface-id</b> command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. <a href="#">Table 2-44</a> describes the fields in this display.
-----------------	--

```
Switch# show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

**Table 0-17 show udld Field Descriptions**

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.

**Table 0-17 show udld Field Descriptions (continued)**

Field	Description
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

■ **show udld**

Related Commands	Command	Description
	<b>udld</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	<b>udld port</b>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.
	<b>udld reset</b>	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

# show version

Use the **show version** command in EXEC mode to display version information for the hardware and firmware.

## show version

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

**Command Modes** User EXEC  
Privileged EXEC

## Command History

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



**Note**

Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

**show vlan**

## show vlan

Use the **show vlan** command in EXEC mode to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

**show vlan [brief | id *vlan-id* | mtu | name *vlan-name* | remote-span | summary]**

Syntax Description		
	<b>brief</b>	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
	<b>id <i>vlan-id</i></b>	(Optional) Display information about a single VLAN identified by VLAN ID number. For <i>vlan-id</i> , the range is 1 to 4094.
	<b>mtu</b>	(Optional) Display a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
	<b>name <i>vlan-name</i></b>	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
	<b>remote-span</b>	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
	<b>summary</b>	(Optional) Display VLAN summary information.

### Command Modes

User EXEC  
Privileged EXEC

### Command History

#### Usage Guidelines

In the **show vlan mtu** command output, the MTU\_Mismatch column shows whether all the ports in the VLAN have the same MTU. When *yes* appears in this column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI\_MTU column. If the MTU-Mismatch column displays *yes*, the names of the port with the MinMTU and the port with the MaxMTU appear.



Though visible in the command-line help string, the **ifindex** keyword not supported.

### Examples

This is an example of output from the **show vlan** command. [Table 2-45](#) describes the fields in the display.

```
Switch# show vlan
VLAN Name                               Status      Ports
---- -----
<output truncated>

2    VLAN0002                           active
3    VLAN0003                           active

<output truncated>

1000 VLAN1000                          active
1002 fddi-default                      active
1003 token-ring-default                active
```

```

1004 fddinet-default           active
1005 trnet-default            active

VLAN Type SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---
1    enet  100001   1500  -     -     -     -     -     1002  1003
2    enet  100002   1500  -     -     -     -     -     0     0
3    enet  100003   1500  -     -     -     -     -     0     0

<output truncated>

1005 trnet 101005     1500  -     -     -     ibm  -     0     0

Remote SPAN VLANs
-----
Primary Secondary Type          Ports
-----  -----  -----  -----

```

**Table 0-18 show vlan Command Output Fields**

<b>Field</b>	<b>Description</b>
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.
Primary/Secondary/ Type/Ports	

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

```

Switch# show vlan summary
Number of existing VLANs      : 45
Number of existing VTP VLANs  : 45
Number of existing extended VLANs : 0

```

This is an example of output from the **show vlan id** command.

```

Switch# show vlan id 2

```

show vlan

```
VLAN Name          Status    Ports
-----            -----
2     VLAN0200      active   Fa1/3, Fa2/5, Fa2/6
VLAN Type   SAID      MTU      Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----            -----  -----  -----  -----  -----  -----  -----  -----
2     enet    100002    1500     -       -       -       -       0       0

Remote SPAN VLAN
-----
Disabled
```

#### Related Commands

Command	Description
<a href="#">switchport mode</a>	Configures the VLAN membership mode of a port.
<a href="#">usb-inactivity-timeout</a>	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.

# show vmpls

Use the **show vmpls** command in EXEC mode without keywords to display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, or use the **statistics** keyword to display client-side statistics.

**show vmpls [statistics]**

<b>Syntax Description</b>	<b>statistics</b>	(Optional) Display VQP client-side statistics and counters.
---------------------------	-------------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

## Command History

### Examples

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

```
Switch# show vmpls
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action: other
```

This is an example of output from the **show vmpls statistics** command. [Table 2-46](#) describes each field in the display.

```
Switch# show vmpls statistics
VMPS Client Statistics
-----
VQP Queries: 0
VQP Responses: 0
VMPS Changes: 0
VQP Shutdowns: 0
VQP Denied: 0
VQP Wrong Domain: 0
VQP Wrong Version: 0
VQP Insufficient Resource: 0
```

**Table 0-19** *show vmpls statistics Field Descriptions*

Field	Description
VQP Queries	Number of queries sent by the client to the VMPS.
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.

**show vmps****Table 0-19 show vmps statistics Field Descriptions (continued)**

<b>Field</b>	<b>Description</b>
VQP Shutdowns	Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively re-enable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address (broadcast or multicast frames are delivered to the workstation if the port has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent more queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The VLAN assignment of the port is not changed. The switches send only VMPS Version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>clear vmps statistics</b></a>	Clears the statistics maintained by the VQP client.
<a href="#"><b>vmps reconfirm (privileged EXEC)</b></a>	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
<a href="#"><b>vmps retry</b></a>	Configures the per-server retry count for the VQP client.
<a href="#"><b>vmps server</b></a>	Configures the primary VMPS and up to three secondary servers.

# show vtp

Use the **show vtp** command in EXEC mode to display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters.

**show vtp {counters | devices [conflicts] | interface [interface-id] | password | status}**

## Syntax Description

<b>counters</b>	Display the VTP statistics for the switch.
<b>password</b>	Display the configured VTP password.
<b>devices</b>	Display information about all VTP version 3 devices in the domain. This keyword applies only if the switch is not running VTP version 3.
<b>conflicts</b>	(Optional) Display information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the switch is in VTP transparent or VPT off mode.
<b>interface [interface-id]</b>	Display VTP status and configuration for all interfaces or the specified interface. The <i>interface-id</i> can be a physical interface or a port channel.
<b>status</b>	Display general information about the VTP management domain status.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.2(52)SE	The <b>devices</b> and <b>interface</b> keywords were added for VTP version 3.

## Usage Guidelines

When you enter the **show vtp password** command when the switch is running VTP version 3, the display follows these rules:

- If the **password password** global configuration command did not specify the **hidden** keyword and encryption is not enabled on the switch, the password appears in clear text.
- If the **password password** command did not specify the **hidden** keyword and encryption is enabled on the switch, the encrypted password appears.
- If the **password password** command included the **hidden** keyword, the hexadecimal secret key is displayed.

## Examples

This is an example of output from the **show vtp devices** command. A **yes** in the *Conflict* column means that the responding server is in conflict with the local server for the feature; that is, when two switches in the same domain do not have the same primary server for a database.

```
Switch# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf switch ID      Primary Server Revision   System Name
          lict
-----
VLAN      Yes  00b0.8e50.d000  000c.0412.6300  12354    main.cisco.com
```

**show vtp**

MST	No	00b0.8e50.d000 0004.AB45.6000 24	main.cisco.com
VLAN	Yes	000c.0412.6300=000c.0412.6300 67	qwertv.cisco.com

This is an example of output from the **show vtp counters** command. [Table 2-47](#) describes the fields in the display.

```
Switch# show vtp counters
```

VTP statistics:

Summary advertisements received	:	0
Subset advertisements received	:	0
Request advertisements received	:	0
Summary advertisements transmitted	:	6970
Subset advertisements transmitted	:	0
Request advertisements transmitted	:	0
Number of config revision errors	:	0
Number of config digest errors	:	0
Number of V1 summary errors	:	0

VTP pruning statistics:

Trunk	Join Transmitted	Join Received	Summary advts received from non-pruning-capable device
Fa0/47	0	0	0
Fa0/48	0	0	0
Gi0/1	0	0	0
Gi0/2	0	0	0

**Table 0-20** **show vtp counters Field Descriptions**

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.

**Table 0-20** show vtp counters Field Descriptions (continued)

Field	Description
Number of configuration revision errors	<p>Number of revision errors.</p> <p>Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments.</p> <p>Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations.</p> <p>These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of configuration digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same.</p> <p>These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of V1 summary errors	<p>Number of Version 1 errors.</p> <p>Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors mean that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.</p>
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command for a switch running VTP version 2. [Table 2-48](#) describes the fields in the display.

```
Switch# show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs : 45
VTP Operating Mode : Transparent
VTP Domain Name : shared_testbed1
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Enabled
MD5 digest : 0x3A 0x29 0x86 0x39 0xB4 0x5D 0x58 0xD7
```

show vtp

**Table 0-21** show vtp status Field Descriptions

Field	Description
VTP Version	Displays the VTP version operating on the switch. By default, the switch implements Version 1 but can be set to Version 2.
Configuration Revision	Current configuration revision number on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every switch is a VTP server.</p> <p><b>Note</b> The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p> <p>Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p>Transparent: a switch in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP V2 Mode	Displays if VTP Version 2 mode is enabled. All VTP Version 2 switches operate in Version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to Version 2 only if all VTP switches in the network can operate in Version 2 mode.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

This is an example of output from the **show vtp status** command for a switch running VTP version 3. .

```
Switch# show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 3
VTP Domain Name          : Cisco
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0021.1bcd.c700
```

```

Feature VLAN:
-----
VTP Operating Mode      : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision   : 0
Primary ID               : 0000.0000.0000
Primary Description       :
MD5 digest              : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                           0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
-----
VTP Operating Mode      : Client
Configuration Revision   : 0
Primary ID               : 0000.0000.0000
Primary Description       :
MD5 digest              : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
                           0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
-----
VTP Operating Mode      : Transparent

```

Related Commands	Command	Description
	<a href="#">clear vtp counters</a>	Clears the VTP and pruning counters.
	<a href="#">vtp (global configuration)</a>	Configures the VTP filename, interface name, domain name, and mode.

# shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled interface.

**shutdown**

**no shutdown**

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

**Defaults** The port is enabled (not shut down).

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

The **shutdown** command causes a port to stop forwarding. You can enable the port with the **no shutdown** command.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

The **shutdown** command disables all functions on the specified interface.

This command also marks the interface as unavailable. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

**Examples** These examples show how to disable and re-enable a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown
```

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

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

### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays the statistical information specific to all interfaces or to a specific interface.

# shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

**shutdown vlan *vlan-id***

**no shutdown vlan *vlan-id***

---

<b>Syntax Description</b>	<i>vlan-id</i> ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs under the VLAN Trunking Protocol (VTP), as well as extended-range VLANs (greater than 1005) cannot be shut down. The default VLANs are 1 and 1002 to 1005.
---------------------------	--

---

<b>Defaults</b>	No default is defined.
-----------------	------------------------

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

## Command History

<b>Usage Guidelines</b>	The <b>shutdown vlan</b> command does not change the VLAN information in the VTP database. The command shuts down local traffic, but the switch still advertises VTP information.
-------------------------	---

<b>Examples</b>	This example shows how to shut down traffic on VLAN 2:
-----------------	--

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

You can verify your setting by entering the **show vlan** privileged EXEC command.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>shutdown (VLAN configuration mode)</b>	Shuts down local traffic on the VLAN when in VLAN configuration mode (accessed by the <b>vlan <i>vlan-id</i></b> global configuration command).

---

**small-frame violation rate**

# small-frame violation rate

Use the **small-frame violation rate *pps*** interface configuration command to configure the rate (threshold) for an interface to be error disabled when it receives VLAN-tagged packets that are small frames (67 bytes or less) at the specified rate. Use the **no** form of this command to return to the default setting.

**small-frame violation rate *pps***

**no small-frame violation rate *pps***

<b>Syntax Description</b>	<i>pps</i>	Specify the threshold at which an interface receiving small frames will be error disabled. The range is 1 to 10,000 packets per second (pps).
---------------------------	------------	---

<b>Defaults</b>	This feature is disabled.
-----------------	---------------------------

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(44)SE	This command was introduced.

<b>Usage Guidelines</b>	This command enables the rate (threshold) for a port to be error disabled when it receives small frames. Small frames are considered packets that are 67 frames or less.
-------------------------	--

Use the **errdisable detect cause small-frame** global configuration command to globally enable the small-frames threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** global configuration command.

<b>Examples</b>	This example shows how to enable the small-frame arrival rate feature so that the port is error disabled if incoming small frames arrived at 10,000 pps.
-----------------	--

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# small-frame violation rate 10000
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Related Commands	Command	Description
	<b>errdisable detect cause small-frame</b>	Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the minimum size and arrives at the specified rate (threshold).
	<b>errdisable recovery cause small-frame</b>	Enables the recovery timer.
	<a href="#">show interfaces</a>	Displays the interface settings on the switch, including input and output flow control.

---

 snmp-server enable traps
 

---

## snmp-server enable traps

Use the **snmp-server enable traps** global configuration command 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 **no** form of this command to return to the default setting.

```
snmp-server enable traps [bridge [newroot] [topologychange] | cluster | config | copy-config |
cpu threshold | entity | envmon [fan | shutdown | status | supply | temperature] | errdisable
[notification-rate value] | flash | ipmulticast | mac-notification [change] [move] [threshold]
| msdp | ospf [cisco-specific | errors | lsa | rate-limit | retransmit | state-change] | pim
[invalid-pim-message | neighbor-change | rp-mapping-change] | port-security [trap-rate
value] | power-ethernet {group name | police} | rtr | snmp [authentication | coldstart |
linkdown | linkup | warmstart] | storm-control trap-rate value | stpx [inconsistency]
[root-inconsistency] [loop-inconsistency] | syslog | tty | vlan-membership | vlancreate |
vlandelete | vtp]

no snmp-server enable traps [bridge [newroot] [topologychange] | cluster | config | copy-config |
cpu threshold | entity | envmon [fan | shutdown | status | supply | temperature] | errdisable
[notification-rate] | flash | ipmulticast | mac-notification [change] [move] [threshold] |
msdp | ospf [cisco-specific | errors | lsa | rate-limit | retransmit | state-change] | pim
[invalid-pim-message | neighbor-change | rp-mapping-change] | port-security [trap-rate]
| power-ethernet {group name | police} | rtr | snmp [authentication | coldstart | linkdown |
linkup | warmstart] | storm-control trap-rate | stpx [inconsistency] [root-inconsistency]
[loop-inconsistency] | syslog | tty | vlan-membership | vlancreate | vlandelete | vtp]
```

Syntax Description	
<b>bridge [newroot] [topologychange]</b>	(Optional) Generate STP bridge MIB traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>newroot</b>—(Optional) Enable SNMP STP Bridge MIB new root traps.</li> <li>• <b>topologychange</b>—(Optional) Enable SNMP STP Bridge MIB topology change traps.</li> </ul>
<b>cluster</b>	(Optional) Enable cluster traps.
<b>config</b>	(Optional) Enable SNMP configuration traps.
<b>copy-config</b>	(Optional) Enable SNMP copy-configuration traps.
<b>cpu threshold</b>	(Optional) Allow CPU-related traps.
<b>entity</b>	(Optional) Enable SNMP entity traps.
<b>envmon [fan   shutdown   status   supply   temperature]</b>	Optional) Enable SNMP environmental traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>fan</b>—(Optional) Enable fan traps.</li> <li>• <b>shutdown</b>—(Optional) Enable environmental monitor shutdown traps.</li> <li>• <b>status</b>—(Optional) Enable SNMP environmental status-change traps.</li> <li>• <b>supply</b>—(Optional) Enable environmental monitor power-supply traps.</li> <li>• <b>temperature</b>—(Optional) Enable environmental monitor temperature traps.</li> </ul>
<b>errdisable [notification-rate value]</b>	(Optional) Enable errdisable traps. Use notification-rate keyword to set the maximum value of errdisable traps sent per minute. The range is 0 to 10000; the default is 0 (no limit imposed; a trap is sent at every occurrence).

<b>flash</b>	(Optional) Enable SNMP FLASH notifications.
<b>ipmulticast</b>	(Optional) Enable IP multicast routing traps.
<b>mac-notification</b>	(Optional) Enable MAC address notification traps.
<b>change</b>	(Optional) Enable MAC address change notification traps.
<b>move</b>	(Optional) Enable MAC address move notification traps.
<b>threshold</b>	(Optional) Enable MAC address table threshold traps.
<b>msdp</b>	(Optional) Enable Multicast Source Discovery Protocol (MSDP) traps.
<b>ospf [cisco-specific   errors   lsa   rate-limit   retransmit   state-change]</b>	(Optional) Enable Open Shortest Path First (OSPF) traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>cisco-specific</b>—(Optional) Enable Cisco-specific traps.</li> <li>• <b>errors</b>—(Optional) Enable error traps.</li> <li>• <b>lsa</b>—(Optional) Enable link-state advertisement (LSA) traps.</li> <li>• <b>rate-limit</b>—(Optional) Enable rate-limit traps.</li> <li>• <b>retransmit</b>—(Optional) Enable packet-retransmit traps.</li> <li>• <b>state-change</b>—(Optional) Enable state-change traps.</li> </ul>
<b>pim [invalid-pim-message   neighbor-change   rp-mapping-change]</b>	(Optional) Enable Protocol-Independent Multicast (PIM) traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>invalid-pim-message</b>—(Optional) Enable invalid PIM message traps.</li> <li>• <b>neighbor-change</b>—(Optional) Enable PIM neighbor-change traps.</li> <li>• <b>rp-mapping-change</b>—(Optional) Enable rendezvous point (RP)-mapping change traps.</li> </ul>
<b>port-security [trap-rate value]</b>	(Optional) Enable port security traps. Use the <b>trap-rate</b> keyword to set 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).
<b>power-ethernet {group name   police}</b>	(Optional) Enable power-over-Ethernet traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>group name</b>—Enable inline power group-based traps for the specified group number or list.</li> <li>• <b>police</b>—Enable inline power policing traps.</li> </ul>
<b>rtr</b>	(Optional) Enable SNMP Response Time Reporter traps.
<b>snmp [authentication   coldstart   linkdown   linkup   warmstart]</b>	(Optional) Enable SNMP traps. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>authentication</b>—(Optional) Enable authentication trap.</li> <li>• <b>coldstart</b>—(Optional) Enable cold start trap.</li> <li>• <b>linkdown</b>—(Optional) Enable linkdown trap.</li> <li>• <b>linkup</b>—(Optional) Enable linkup trap.</li> <li>• <b>warmstart</b>—(Optional) Enable warmstart trap.</li> </ul>
<b>storm-control trap-rate value</b>	(Optional) Enable storm-control traps. Use the <b>trap-rate</b> keyword to set the maximum number of storm-control traps sent per minute. The range is 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).

**■ snmp-server enable traps**


---

<b>stpx</b>	(Optional) Enable SNMP STPX MIB traps. The keywords have these meanings:
	<ul style="list-style-type: none"> <li>• <b>inconsistency</b>—(Optional) Enable SNMP STPX MIB Inconsistency Update traps.</li> <li>• <b>root-inconsistency</b>—(Optional) Enable SNMP STPX MIB Root Inconsistency Update traps.</li> <li>• <b>loop-inconsistency</b>—(Optional) Enable SNMP STPX MIB Loop Inconsistency Update traps.</li> </ul>
<b>syslog</b>	(Optional) Enable SNMP syslog traps.
<b>tty</b>	(Optional) Send TCP connection traps. This is enabled by default.
<b>vlan-membership</b>	(Optional) Enable SNMP VLAN membership traps.
<b>vlancreate</b>	(Optional) Enable SNMP VLAN-created traps.
<b>vlandelete</b>	(Optional) Enable SNMP VLAN-deleted traps.
<b>vtp</b>	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

---

**Note**

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.

**Defaults**

The sending of SNMP traps is disabled.

**Command Modes**

Global configuration

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(37)SE	The <b>errdisable notification-rate value</b> keywords were added.
12.2(40)SE	The <b>change</b> , <b>move</b> , and <b>threshold</b> keywords were added to the mac-notification option.
12.2(44)SE	The <b>power-ethernet {group name   police}</b> keywords were added.
12.2(50)SE	The <b>cpu threshold</b> keywords were added.

**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 types are sent.

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

**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.

To set the CPU threshold notification types and values, use the **process cpu threshold type** global configuration command.

**Examples**

This example shows how to send VTP traps to the NMS:

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

You can verify your setting by entering the **show vtp status** or the **show running-config** privileged EXEC command.

**Related Commands**

Command	Description
<b>show running-config</b>	Displays the running configuration on the switch.
<b>snmp-server host</b>	Specifies the host that receives SNMP traps.

**snmp-server host**

## snmp-server host

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

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

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

---

Syntax Description	
<b>host-addr</b>	Name or Internet address of the host (the targeted recipient).
<b>udp-port</b> <i>port</i>	(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is 0 to 65535.
<b>informs</b>   <b>traps</b>	(Optional) Send SNMP traps or informs to this host.
<b>version</b> <b>1</b>   <b>2c</b>   <b>3</b>	(Optional) Version of the SNMP used to send the traps.  These keywords are supported: <b>1</b> —SNMPv1. This option is not available with informs. <b>2c</b> —SNMPv2C. <b>3</b> —SNMPv3. These optional keywords can follow the Version 3 keyword: <ul style="list-style-type: none"><li>• <b>auth</b> (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</li><li>• <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.</li><li>• <b>priv</b> (Optional). Enables Data Encryption Standard (DES) packet encryption (also called <i>privacy</i>).</li></ul>
<b>vrf</b> <i>vrf-instance</i>	(Optional) Virtual private network (VPN) routing instance and name for this host.
<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 <b>priv</b> keyword is available only when the cryptographic (encrypted) software image is installed.

---

---

<i>notification-type</i>	(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: <ul style="list-style-type: none"><li>• <b>bridge</b>—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps.</li><li>• <b>cluster</b>—Send cluster member status traps.</li><li>• <b>config</b>—Send SNMP configuration traps.</li><li>• <b>copy-config</b>—Send SNMP copy configuration traps.</li><li>• <b>cpu threshold</b>—Allow CPU-related traps.</li><li>• <b>entity</b>— Send SNMP entity traps.</li><li>• <b>envmon</b>—Send environmental monitor traps.</li><li>• <b>errdisable</b>—Send SNMP errdisable notifications.</li><li>• <b>flash</b>—Send SNMP FLASH notifications.</li><li>• <b>hsrp</b>—Send SNMP Hot Standby Router Protocol (HSRP) traps.</li><li>• <b>ipmulticast</b>—Send SNMP IP multicast routing traps.</li><li>• <b>mac-notification</b>—Send SNMP MAC notification traps.</li><li>• <b>msdp</b>—Send SNMP Multicast Source Discovery Protocol (MSDP) traps.</li><li>• <b>ospf</b>—Send Open Shortest Path First (OSPF) traps.</li><li>• <b>pim</b>—Send SNMP Protocol-Independent Multicast (PIM) traps.</li><li>• <b>port-security</b>—Send SNMP port-security traps.</li><li>• <b>rtr</b>—Send SNMP Response Time Reporter traps.</li><li>• <b>snmp</b>—Send SNMP-type traps.</li><li>• <b>storm-control</b>—Send SNMP storm-control traps.</li><li>• <b>stpx</b>—Send SNMP STP extended MIB traps.</li><li>• <b>syslog</b>—Send SNMP syslog traps.</li><li>• <b>tty</b>—Send TCP connection traps.</li><li>• <b>udp-port</b> <i>port</i>—Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535.</li><li>• <b>vlan-membership</b>— Send SNMP VLAN membership traps.</li><li>• <b>vlancreate</b>—Send SNMP VLAN-created traps.</li><li>• <b>vlandelete</b>—Send SNMP VLAN-deleted traps.</li><li>• <b>vtp</b>—Send SNMP VLAN Trunking Protocol (VTP) traps.</li></ul>
--------------------------	---

---

**snmp-server host****Defaults**

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.

**Command Modes**

Global configuration

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(37)SE	The <b>errdisable notification-rate value</b> keywords were added.
12.2(50)SE	The <b>cpu threshold</b> keywords were added.

**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. Thus, 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**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the running configuration on the switch.
<b>snmp-server enable traps</b>	Enables SNMP notification for various trap types or inform requests.

---

 ■ **snmp trap mac-notification change**

# snmp trap mac-notification change

Use the **snmp trap mac-notification change** interface configuration command to enable the Simple Network Management Protocol (SNMP) MAC address change notification trap on a specific Layer 2 interface. Use the **no** form of this command to return to the default setting.

**snmp trap mac-notification change {added | removed}**

**no snmp trap mac-notification change {added | removed}**

<b>Syntax Description</b>	<b>added</b> Enable the MAC notification trap when a MAC address is added on this interface. <b>removed</b> Enable the MAC notification trap when a MAC address is removed from this interface.
---------------------------	--

---

**Defaults** By default, the traps for both address addition and address removal are disabled.

---

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(40)SE	The word <b>change</b> was added to the command.

---

**Usage Guidelines** Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification change** command, the trap is generated only when you enter the **snmp-server enable traps mac-notification change** and the **mac address-table notification change** global configuration commands.

---

**Examples** This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

You can verify your settings by entering the **show mac address-table notification change interface** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">clear mac address-table notification</a>	Clears the MAC address notification global counters.
	<a href="#">mac address-table notification</a>	Enables the MAC address notification feature.
	<a href="#">show mac address-table notification</a>	Displays the MAC address notification settings for all interfaces or on the specified interface when the <b>interface</b> keyword is appended.
	<a href="#">snmp-server enable traps</a>	Sends the SNMP MAC notification traps when the <b>mac-notification</b> keyword is appended.

**spanning-tree backbonefast**

# spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of the command to return to the default setting.

**spanning-tree backbonefast**

**no spanning-tree backbonefast**

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

**Defaults** BackboneFast is disabled.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

You can configure the BackboneFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

BackboneFast starts when a root port or blocked port on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an *indirect* link) has failed (that is, the designated switch has lost its connection to the root switch). If there are alternate paths to the root switch, BackboneFast causes the maximum aging time on the interfaces on which it received the inferior BPDU to expire and allows a blocked port to move immediately to the listening state. BackboneFast then transitions the interface to the forwarding state. For more information, see the software configuration guide for this release.

Enable BackboneFast on all supported switches to allow the detection of indirect link failures and to start the spanning-tree reconfiguration sooner.

---

### Examples

This example shows how to enable BackboneFast on the switch:

```
Switch(config)# spanning-tree backbonefast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

---

### Related Commands

Command	Description
<a href="#">show spanning-tree summary</a>	Displays a summary of the spanning-tree interface states.

# spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command to prevent an interface from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

**spanning-tree bpdufilter { disable | enable }**

**no spanning-tree bpdufilter**

<b>Syntax Description</b>	<b>disable</b> Disable BPDU filtering on the specified interface. <b>enable</b> Enable BPDU filtering on the specified interface.
---------------------------	--

<b>Defaults</b>	BPDU filtering is disabled.
-----------------	-----------------------------

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

## Command History

## Usage Guidelines

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.



**Caution** Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled interfaces by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

## Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

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

**spanning-tree bpdufilter**

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current operating configuration.
	<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interface or enables the Port Fast feature on all nontrunking interfaces.
	<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface and all its associated VLANs.

# spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command to put an interface in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

**spanning-tree bpduguard { disable | enable }**

**no spanning-tree bpduguard**

<b>Syntax Description</b>	<b>disable</b> Disable BPDU guard on the specified interface. <b>enable</b> Enable BPDU guard on the specified interface.
---------------------------	--

<b>Defaults</b>	BPDU guard is disabled.
-----------------	-------------------------

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

## Command History

**Usage Guidelines** The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled interfaces by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

<b>Examples</b>	This example shows how to enable the BPDU guard feature on a port:
-----------------	--

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

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

**spanning-tree bpduguard**

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current operating configuration.
	<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
	<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface and all its associated VLANs.

# spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree [vlan *vlan-id*] cost *cost***

**no spanning-tree [vlan *vlan-id*] cost**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. <b>cost</b> Path cost. The range is 1 to 200000000, with higher values meaning higher costs.
---------------------------	---

<b>Defaults</b>	The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values: <ul style="list-style-type: none"> <li>• 1000 Mb/s—4</li> <li>• 100 Mb/s—19</li> <li>• 10 Mb/s—100</li> </ul>
-----------------	--

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

## Command History

### Usage Guidelines

When you configure the cost, higher values represent higher costs.

If you configure an interface with both the **spanning-tree vlan *vlan-id* cost *cost*** command and the **spanning-tree cost *cost*** command, the **spanning-tree vlan *vlan-id* cost *cost*** command takes effect.

<b>Examples</b>	This example shows how to set the path cost to 250 on a port:
-----------------	---

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

## Related Commands

**spanning-tree cost**

Command	Description
<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree information for the specified interface.
<b>spanning-tree port-priority</b>	Configures an interface priority.
<b>spanning-tree vlan priority</b>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

**spanning-tree etherchannel guard misconfig**

**no spanning-tree etherchannel guard misconfig**

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

**Defaults** EtherChannel guard is enabled on the switch.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

When the switch detects an EtherChannel misconfiguration, this error message appears:

PM-4-ERR\_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in err-disable state.

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

**Examples** This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

**spanning-tree etherchannel guard misconfig**

Related Commands	Command	Description
	<b>errdisable recovery cause channel-misconfig</b>	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
	<b>show etherchannel summary</b>	Displays EtherChannel information for a channel as a one-line summary per channel-group.
	<b>show interfaces status err-disabled</b>	Displays the interfaces in the error-disabled state.

# spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

## spanning-tree extend system-id



**Note** Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

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

**Defaults** The extended system ID is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
-----------------	---------	--------------

**Usage Guidelines** The switch supports the IEEE 802.1t spanning-tree extensions. Some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and rapid PVST+ or as an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the “[spanning-tree mst root](#)” and the “[spanning-tree vlan](#)” sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

**spanning-tree extend system-id**

Related Commands	Command	Description
	<a href="#">show spanning-tree summary</a>	Displays a summary of spanning-tree interface states.
	<a href="#">spanning-tree mst root</a>	Configures the MST root switch priority and timers based on the network diameter.
	<a href="#">spanning-tree vlan priority</a>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree guard

Use the **spanning-tree guard** interface configuration command to enable root guard or loop guard on all the VLANs associated with the selected interface. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

**spanning-tree guard {loop | none | root}**

**no spanning-tree guard**

Syntax Description	
<b>loop</b>	Enable loop guard.
<b>none</b>	Disable root guard or loop guard.
<b>root</b>	Enable root guard.

## Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected interface. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Do not enable root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state. The UplinkFast feature is not available when the switch is operating in the rapid-PVST+ or MST mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate

**spanning-tree guard**

ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

**Examples**

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the current operating configuration.
<b>spanning-tree cost</b>	Sets the path cost for spanning-tree calculations.
<b>spanning-tree loopguard default</b>	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
<b>spanning-tree mst cost</b>	Configures the path cost for MST calculations.
<b>spanning-tree mst port-priority</b>	Configures an interface priority.
<b>spanning-tree mst root</b>	Configures the MST root switch priority and timers based on the network diameter.
<b>spanning-tree port-priority</b>	Configures an interface priority.
<b>spanning-tree vlan priority</b>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command to override the default link-type setting, which is determined by the duplex mode of the interface, and to enable rapid spanning-tree transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree link-type {point-to-point | shared}**

**no spanning-tree link-type**

<b>Syntax Description</b>	<b>point-to-point</b> Specify that the link type of an interface is point-to-point. <b>shared</b> Specify that the link type of an interface is shared.
---------------------------	--

<b>Defaults</b>	The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.
-----------------	--

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

<b>Command History</b>	
<b>Usage Guidelines</b>	You can override the default setting of the link type by using the <b>spanning-tree link-type</b> command. For example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

<b>Examples</b>	This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:
	Switch(config-if)# <b>spanning-tree link-type shared</b>

You can verify your setting by entering the **show spanning-tree mst interface interface-id** or the **show spanning-tree interface interface-id** privileged EXEC command.

spanning-tree link-type

Related Commands	Command	Description
	<b>clear spanning-tree detected-protocols</b>	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
	<b>show spanning-tree interface</b> <i>interface-id</i>	Displays spanning-tree state information for the specified interface.
	<b>show spanning-tree mst interface</b> <i>interface-id</i>	Displays MST information for the specified interface.

# spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

**spanning-tree loopguard default**

**no spanning-tree loopguard default**

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

**Defaults** Loop guard is disabled.

**Command Modes** Global configuration

## Command History

**Usage Guidelines** You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on interfaces that the spanning tree identifies as point-to-point.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

**Examples** This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

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

## Related Commands

Command	Description
<b>show running-config</b>	Displays the current operating configuration.
<b>spanning-tree guard loop</b>	Enables the loop guard feature on all the VLANs associated with the specified interface.

**spanning-tree mode**

# spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

**spanning-tree mode {mst | pvst | rapid-pvst}**

**no spanning-tree mode**

<b>Syntax Description</b>	<b>mst</b> Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w). <b>pvst</b> Enable PVST+ (based on IEEE 802.1D). <b>rapid-pvst</b> Enable rapid PVST+ (based on IEEE 802.1w).
---------------------------	---

**Defaults**      The default mode is PVST+.

**Command Modes**      Global configuration

## Command History

### Usage Guidelines

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.



**Caution**      Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

### Examples

This example shows to enable MST and RSTP on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable rapid PVST+ on the switch:

```
Switch(config)# spanning-tree mode rapid-pvst
```

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the current operating configuration.

# spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

## **spanning-tree mst configuration**

### **no spanning-tree mst configuration**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	The default mapping is that all VLANs are mapped to the common and internal spanning-tree (CIST) instance (instance 0).
-----------------	---

The default name is an empty string.

The revision number is 0.

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

## **Command History**

### **Usage Guidelines**

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance *instance-id* *vlan* *vlan-range***: maps VLANs to an MST instance. The range for the *instance-id* is 1 to 4094. The range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name *name***: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Though visible in the command-line help strings, this command is not supported.
- **revision *version***: sets the configuration revision number. The range is 0 to 65535.
- **show [current | pending]**: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

**spanning-tree mst configuration**

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

**Examples**

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
-----
0        1-9,21-4094
1        10-20
-----
Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show spanning-tree mst configuration</b></a>	Displays the MST region configuration.

# spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree mst *instance-id* cost *cost***

**no spanning-tree mst *instance-id* cost**

Syntax Description	<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
	<i>cost</i>	Path cost is 1 to 200000000, with higher values meaning higher costs.

**Defaults** The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mb/s—20000
- 100 Mb/s—200000
- 10 Mb/s—2000000

**Command Modes** Interface configuration

## Command History

**Usage Guidelines** When you configure the cost, higher values represent higher costs.

**Examples** This example shows how to set a path cost of 250 on a port associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

You can verify your settings by entering the **show spanning-tree mst interface *interface-id*** privileged EXEC command.

**spanning-tree mst cost**

Related Commands	Command	Description
	<b>show spanning-tree mst interface <i>interface-id</i></b>	Displays MST information for the specified interface.
	<b>spanning-tree mst port-priority</b>	Configures an interface priority.
	<b>spanning-tree mst priority</b>	Configures the switch priority for the specified spanning-tree instance.

# spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

**spanning-tree mst forward-time *seconds***

**no spanning-tree mst forward-time**

<b>Syntax Description</b>	<i>seconds</i> Length of the listening and learning states. The range is 4 to 30 seconds.										
<b>Defaults</b>	The default is 15 seconds.										
<b>Command Modes</b>	Global configuration										
<b>Command History</b>											
<b>Usage Guidelines</b>	Changing the <b>spanning-tree mst forward-time</b> command affects all spanning-tree instances.										
<b>Examples</b>	<p>This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:</p> <pre>Switch(config)# spanning-tree mst forward-time 18</pre> <p>You can verify your setting by entering the <b>show spanning-tree mst</b> privileged EXEC command.</p>										
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><a href="#">show spanning-tree mst</a></td><td>Displays MST information.</td></tr> <tr> <td><a href="#">spanning-tree mst hello-time</a></td><td>Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.</td></tr> <tr> <td><a href="#">spanning-tree mst max-age</a></td><td>Sets the interval between messages that the spanning tree receives from the root switch.</td></tr> <tr> <td><a href="#">spanning-tree mst max-hops</a></td><td>Sets the number of hops in a region before the BPDU is discarded.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">show spanning-tree mst</a>	Displays MST information.	<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.
<b>Command</b>	<b>Description</b>										
<a href="#">show spanning-tree mst</a>	Displays MST information.										
<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.										
<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.										
<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.										

**spanning-tree mst hello-time**

# spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

**spanning-tree mst hello-time *seconds***

**no spanning-tree mst hello-time**

<b>Syntax Description</b>	<i>seconds</i>	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
---------------------------	----------------	--

<b>Defaults</b>	The default is 2 seconds.
-----------------	---------------------------

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

## Command History

<b>Usage Guidelines</b>	After you set the <b>spanning-tree mst max-age</b> <i>seconds</i> global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The <b>max-age</b> setting must be greater than the <b>hello-time</b> setting. Changing the <b>spanning-tree mst hello-time</b> command affects all spanning-tree instances.
-------------------------	---

<b>Examples</b>	This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:
-----------------	---

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst max-age</a>	Sets the interval between messages that the spanning tree receives from the root switch.
	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.

# spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-age *seconds***

**no spanning-tree mst max-age**

<b>Syntax Description</b>	<i>seconds</i> Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.
---------------------------	---

<b>Defaults</b>	The default is 20 seconds.
-----------------	----------------------------

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

## Command History

<b>Usage Guidelines</b>	After you set the <b>spanning-tree mst max-age <i>seconds</i></b> global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The <b>max-age</b> setting must be greater than the <b>hello-time</b> setting. Changing the <b>spanning-tree mst max-age</b> command affects all spanning-tree instances.
-------------------------	--

<b>Examples</b>	This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:
-----------------	---

```
Switch(config)# spanning-tree mst max-age 30
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst</a>	Displays MST information.
	<a href="#">spanning-tree mst forward-time</a>	Sets the forward-delay time for all MST instances.
	<a href="#">spanning-tree mst hello-time</a>	Sets the interval between hello BPDUs sent by root switch configuration messages.
	<a href="#">spanning-tree mst max-hops</a>	Sets the number of hops in a region before the BPDU is discarded.

**spanning-tree mst max-hops**

# spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-hops *hop-count***

**no spanning-tree mst max-hops**

<b>Syntax Description</b>	<i>hop-count</i> Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.
---------------------------	---

<b>Defaults</b>	The default is 20 hops.
-----------------	-------------------------

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

## Command History

**Usage Guidelines** The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the interface when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

<b>Examples</b>	This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:
-----------------	--

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands	Command	Description
	<b>show spanning-tree mst</b>	Displays MST information.
	<b>spanning-tree mst forward-time</b>	Sets the forward-delay time for all MST instances.
	<b>spanning-tree mst hello-time</b>	Sets the interval between hello BPDUs sent by root switch configuration messages.
	<b>spanning-tree mst max-age</b>	Sets the interval between messages that the spanning tree receives from the root switch.

---

spanning-tree mst port-priority

# spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree mst *instance-id* port-priority *priority***

**no spanning-tree mst *instance-id* port-priority**

<b>Syntax Description</b>	<p><i>instance-id</i> Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</p> <p><i>priority</i> The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.</p>
---------------------------	---

---

**Defaults**

The default is 128.

---

**Command Modes**

Interface configuration

---

**Command History**
**Usage Guidelines**

You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

---

**Examples**

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface *interface-id*** privileged EXEC command.

---

**Related Commands**

Command	Description
<b>show spanning-tree mst interface <i>interface-id</i></b>	Displays MST information for the specified interface.
<b>spanning-tree mst cost</b>	Sets the path cost for MST calculations.
<b>spanning-tree mst priority</b>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree mst pre-standard

Use the **spanning-tree mst pre-standard** interface configuration command to configure a port to send only prestandard bridge protocol data units (BPDUs).

**spanning-tree mst pre-standard**

**no spanning-tree mst pre-standard**

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

**Command Default** The default state is automatic detection of prestandard neighbors.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines



The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.

---

If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

### Examples

This example shows how to configure a port to send only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

### Related Commands

Command	Description
<b>show spanning-tree mst instance-id</b>	Displays multiple spanning-tree (MST) information, including the <i>prestandard</i> flag, for the specified interface.

**spanning-tree mst priority**

# spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

**spanning-tree mst *instance-id* priority *priority***

**no spanning-tree mst *instance-id* priority**

<b>Syntax Description</b>	<p><i>instance-id</i> Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</p> <p><b>priority</b> Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.</p> <p>The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.</p>
---------------------------	---

<b>Defaults</b>	The default is 32768.
<b>Command Modes</b>	Global configuration

<b>Command History</b>	
<b>Examples</b>	This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show spanning-tree mst <i>instance-id</i></a>	Displays MST information for the specified interface.
	<a href="#">spanning-tree mst cost</a>	Sets the path cost for MST calculations.
	<a href="#">spanning-tree mst port-priority</a>	Configures an interface priority.

# spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

**spanning-tree mst *instance-id* root {primary | secondary} [diameter *net-diameter* [hello-time *seconds*]]]**

**no spanning-tree mst *instance-id* root**

Syntax Description		
	<i>instance-id</i>	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
	<b>root primary</b>	Force this switch to be the root switch.
	<b>root secondary</b>	Set this switch to be the root switch should the primary root switch fail.
	<b>diameter <i>net-diameter</i></b>	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
	<b>hello-time <i>seconds</i></b>	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

## Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

Use the **spanning-tree mst *instance-id* root** command only on backbone switches.

When you enter the **spanning-tree mst *instance-id* root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst *instance-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

**spanning-tree mst root****Examples**

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst *instance-id*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show spanning-tree mst <i>instance-id</i></b></a>	Displays MST information for the specified instance.
<a href="#"><b>spanning-tree mst forward-time</b></a>	Sets the forward-delay time for all MST instances.
<a href="#"><b>spanning-tree mst hello-time</b></a>	Sets the interval between hello BPDUs sent by root switch configuration messages.
<a href="#"><b>spanning-tree mst max-age</b></a>	Sets the interval between messages that the spanning tree receives from the root switch.
<a href="#"><b>spanning-tree mst max-hops</b></a>	Sets the number of hops in a region before the BPDU is discarded.

# spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to configure an interface priority. If a loop occurs, spanning tree can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree [vlan *vlan-id*] port-priority *priority***

**no spanning-tree [vlan *vlan-id*] port-priority**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. <b>priority</b> Number from 0 to 240, in increments of 16. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.
---------------------------	--

**Defaults**      The default is 128.

**Command Modes**      Interface configuration

## Command History

**Usage Guidelines**      If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the interface to the VLAN.

If you configure an interface with both the **spanning-tree vlan *vlan-id* port-priority *priority*** command and the **spanning-tree port-priority *priority*** command, the **spanning-tree vlan *vlan-id* port-priority *priority*** command takes effect.

**spanning-tree port-priority****Examples**

This example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface *interface-id*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show spanning-tree interface</b></a> <i>interface-id</i>	Displays spanning-tree information for the specified interface.
<a href="#"><b>spanning-tree cost</b></a>	Sets the path cost for spanning-tree calculations.
<a href="#"><b>spanning-tree vlan priority</b></a>	Sets the switch priority for the specified spanning-tree instance.

# spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled interfaces, the BPDU guard feature on Port Fast-enabled interfaces, or the Port Fast feature on all nontrunking interfaces. The BPDU filtering feature prevents the switch interface from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled interfaces that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default settings.

**spanning-tree portfast {bpdufilter default | bpduguard default | default}**

**no spanning-tree portfast {bpdufilter default | bpduguard default | default}**

Syntax Description		
	<b>bpdufilter default</b>	Globally enable BPDU filtering on Port Fast-enabled interfaces and prevent the switch interface connected to end stations from sending or receiving BPDUs.
	<b>bpduguard default</b>	Globally enable the BPDU guard feature on Port Fast-enabled interfaces and place the interfaces that receive BPDUs in an error-disabled state.
	<b>default</b>	Globally enable the Port Fast feature on all nontrunking interfaces. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

## Defaults

The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all interfaces unless they are individually configured.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+) rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on interfaces that are Port Fast-enabled (the interfaces are in a Port Fast-operational state). The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** global configuration command by using the **spanning-tree bpdufilter** interface configuration command.



### Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

**spanning-tree portfast (global configuration)**

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on interfaces that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled interfaces do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled interface signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the interface in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bpduguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. Configure Port Fast only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled interface moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all interfaces unless they are individually configured with the **spanning-tree portfast** interface configuration command.

**Examples**

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the current operating configuration.
<b>spanning-tree bpdufilter</b>	Prevents an interface from sending or receiving BPDUs.
<b>spanning-tree bpduguard</b>	Puts an interface in the error-disabled state when it receives a BPDU.
<b>spanning-tree portfast (interface configuration)</b>	Enables the Port Fast feature on an interface in all its associated VLANs.

# spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on an interface in all its associated VLANs. When the Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

**spanning-tree portfast [disable | trunk]**

**no spanning-tree portfast**

<b>Syntax Description</b>	<b>disable</b> (Optional) Disable the Port Fast feature on the specified interface. <b>trunk</b> (Optional) Enable the Port Fast feature on a trunking interface.
---------------------------	--

<b>Defaults</b>	The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.
-----------------	--

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

## Command History

### Usage Guidelines

Use this feature only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the interface.

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an interface that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

**spanning-tree portfast (interface configuration)****Examples**

This example shows how to enable the Port Fast feature on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the current operating configuration.
<b>spanning-tree bpdufilter</b>	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
<b>spanning-tree bpduguard</b>	Puts an interface in the error-disabled state when it receives a BPDU.
<b>spanning-tree portfast (global configuration)</b>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.

# spanning-tree transmit hold-count

Use the **spanning-tree transmit hold-count** global configuration command to configure the number of bridge protocol data units (BPDUs) sent every second. Use the **no** form of this command to return to the default setting.

**spanning-tree transmit hold-count [value]**

**no spanning-tree transmit hold-count [value]**

<b>Syntax Description</b>	<i>value</i> (Optional) Number of BPDUs sent every second. The range is 1 to 20.				
<b>Defaults</b>	The default is 6.				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>					
<b>Usage Guidelines</b>	Increasing the transmit hold-count value can have a significant impact on CPU utilization when the switch is in rapid-per-VLAN spanning-tree plus (rapid-PVST+) mode. Decreasing this value might slow down convergence. We recommend using the default setting.				
<b>Examples</b>	<p>This example shows how to set the transmit hold count to 8:</p> <pre>Switch(config)# <b>spanning-tree transmit hold-count 8</b></pre> <p>You can verify your setting by entering the <b>show spanning-tree mst</b> privileged EXEC command.</p>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><a href="#">show spanning-tree mst</a></td><td>Displays the multiple spanning-tree (MST) region configuration and status, including the transmit hold count.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">show spanning-tree mst</a>	Displays the multiple spanning-tree (MST) region configuration and status, including the transmit hold count.
<b>Command</b>	<b>Description</b>				
<a href="#">show spanning-tree mst</a>	Displays the multiple spanning-tree (MST) region configuration and status, including the transmit hold count.				

**spanning-tree uplinkfast**

# spanning-tree uplinkfast

Use the **spanning-tree uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

**spanning-tree uplinkfast [max-update-rate *pkts-per-second*]**

**no spanning-tree uplinkfast [max-update-rate]**

<b>Syntax Description</b>	<b>max-update-rate <i>pkts-per-second</i></b>	(Optional) The number of packets per second at which update packets are sent. The range is 0 to 32000.
---------------------------	---	--

**Defaults** UplinkFast is disabled.

The update rate is 150 packets per second.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

Use this command only on access switches.

You can configure the UplinkFast feature for rapid PVST+ or for multiple spanning-tree (MST) mode, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduces the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When spanning tree detects that the root port has failed, UplinkFast immediately changes to an alternate root port, changing the new root port directly to forwarding state. During this time, a topology change notification is sent.

Do not enable the root guard on interfaces that will be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and prevented from reaching the forwarding state.

If you set the max-update-rate to 0, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

**Examples**

This example shows how to enable UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

You can verify your setting by entering the **show spanning-tree summary** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">show spanning-tree summary</a>	Displays a summary of the spanning-tree interface states.
<a href="#">spanning-tree vlan root primary</a>	Forces this switch to be the root switch.

**spanning-tree vlan**

# spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time seconds | max-age seconds |
priority priority | root {primary | secondary} [diameter net-diameter |
hello-time seconds]]]
```

```
no spanning-tree vlan vlan-id [forward-time | hello-time | max-age | priority | root]
```

Syntax Description	
<b><i>vlan-id</i></b>	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
<b>forward-time</b> <i>seconds</i>	(Optional) Set the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
<b>hello-time</b> <i>seconds</i>	(Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
<b>max-age</b> <i>seconds</i>	(Optional) Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
<b>priority</b> <i>priority</i>	(Optional) Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.  The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
<b>root primary</b>	(Optional) Force this switch to be the root switch.
<b>root secondary</b>	(Optional) Set this switch to be the root switch should the primary root switch fail.
<b>diameter</b> <i>net-diameter</i>	(Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7.

---

## Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

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

**Command History****Usage Guidelines**

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan *vlan-id*** privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age seconds**, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan *vlan-id* root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan *vlan-id* root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan *vlan-id* root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

**Examples**

This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

**spanning-tree vlan**

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan *vlan-id*** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show spanning-tree vlan</a>	Displays spanning-tree information.
<a href="#">spanning-tree cost</a>	Sets the path cost for spanning-tree calculations.
<a href="#">spanning-tree guard</a>	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
<a href="#">spanning-tree port-priority</a>	Sets an interface priority.
<a href="#">spanning-tree portfast (global configuration)</a>	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
<a href="#">spanning-tree portfast (interface configuration)</a>	Enables the Port Fast feature on an interface in all its associated VLANs.
<a href="#">spanning-tree uplinkfast</a>	Enables the UplinkFast feature, which accelerates the choice of a new root port.

# speed

Use the **speed** interface configuration command to specify the speed of a 10/100 Mb/s or 10/100/1000 Mb/s port. Use the **no** or **default** form of this command to return the port to its default value.

**speed { 10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate }**

**no speed**

Syntax Description	
<b>10</b>	Port runs at 10 Mb/s.
<b>100</b>	Port runs at 100 Mb/s.
<b>1000</b>	Port runs at 1000 Mb/s. This option is valid and visible only on 10/100/1000 Mb/s-ports.
<b>auto</b>	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the <b>10</b> , <b>100</b> , or <b>1000</b> keywords with the <b>auto</b> keyword, the port only autonegotiates at the specified speeds.
<b>nonegotiate</b>	Autonegotiation is disabled, and the port runs at 1000 Mb/s. (The 1000BASE-T SFP does not support the nonegotiate keyword.)

## Defaults

The default is **auto**.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.



**Caution** Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

## Examples

This example shows how to set the speed on a port to 100 Mb/s:

```
Switch(config-if)# speed 100
```

**speed**

This example shows how to set a port to autonegotiate at only 10 Mb/s:

```
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mb/s:

```
Switch(config-if)# speed auto 10 100
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>duplex</b></a>	Specifies the duplex mode of operation.
<a href="#"><b>show interfaces</b></a>	Displays the statistical information specific to all interfaces or to a specific interface.

# srr-queue bandwidth limit

Use the **srr-queue bandwidth limit** interface configuration command to limit the maximum output on a port. Use the **no** form of this command to return to the default setting.

**srr-queue bandwidth limit *weight1***

**no srr-queue bandwidth limit**

<b>Syntax Description</b>	<i>weight1</i> Percentage of the port speed to which the port should be limited. The range is 10 to 90.
<b>Defaults</b>	The port is not rate limited and is set to 100 percent.
<b>Command Modes</b>	Interface configuration
<b>Command History</b>	
<b>Usage Guidelines</b>	If you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed. These values are not exact because the hardware adjusts the line rate in increments of six.
 <b>Note</b>	The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your quality of service (QoS) solution.
<b>Examples</b>	<p>This example shows how to limit a port to 800 Mb/s:</p> <pre>Switch(config)# interface gigabitethernet0/1 Switch(config-if)# srr-queue bandwidth limit 80</pre> <p>You can verify your settings by entering the <b>show mls qos interface [interface-id] queueing</b> privileged EXEC command.</p>

**srr-queue bandwidth limit**

Related Commands	Command	Description
	<b>mls qos queue-set output buffers</b>	Allocates buffers to the queue-set.
	<b>mls qos srr-queue output cos-map</b>	Maps class of service (CoS) values to egress queue or maps CoS values to a queue and to a threshold ID.
	<b>mls qos srr-queue output dscp-map</b>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	<b>mls qos queue-set output threshold</b>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation for the queue-set.
	<b>queue-set</b>	Maps a port to a queue-set.
	<b>show mls qos interface queueing</b>	Displays QoS information.
	<b>srr-queue bandwidth shape</b>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.
	<b>srr-queue bandwidth share</b>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

# srr-queue bandwidth shape

Use the **srr-queue bandwidth shape** interface configuration command to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port. Use the **no** form of this command to return to the default setting.

**srr-queue bandwidth shape weight1 weight2 weight3 weight4**

**no srr-queue bandwidth shape**

Syntax Description	weight1 weight2 weight3 weight4	Specify the weights to specify the percentage of the port that is shaped. The inverse ratio (1/weight) specifies the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.
--------------------	------------------------------------	---

**Defaults** Weight1 is set to 25. Weight2, weight3, and weight4 are set to 0, and these queues are in shared mode.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

In shaped mode, the queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Use shaping to smooth bursty traffic or to provide a smoother output over time.

The shaped mode overrides the shared mode.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue come into effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.



### Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

## Examples

This example shows how to configure the queues for the same port for both shaping and sharing. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent. Queue 1 is guaranteed this bandwidth and limited to it; it does not extend its slot to the other queues even if the other queues have no traffic and are idle. Queues 2, 3, and 4 are in shared mode, and the setting for queue 1 is ignored. The bandwidth ratio allocated for the queues in shared mode is 4/(4+4+4), which is 33 percent:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

**srr-queue bandwidth shape**

```
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

You can verify your settings by entering the **show mls qos interface [interface-id] queueing** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
	<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue output dscp-map</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	<a href="#">priority-queue</a>	Enables the egress expedite queue on a port.
	<a href="#">queue-set</a>	Maps a port to a queue-set.
	<a href="#">show mls qos interface queueing</a>	Displays quality of service (QoS) information.
	<a href="#">srr-queue bandwidth share</a>	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.

# srr-queue bandwidth share

Use the **srr-queue bandwidth share** interface configuration command switch to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. The ratio of the weights is the ratio of frequency in which the shaped round robin (SRR) scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

**srr-queue bandwidth share weight1 weight2 weight3 weight4**

**no srr-queue bandwidth share**

Syntax Description	<i>weight1 weight2 weight3 weight4</i>	The ratios of <i>weight1</i> , <i>weight2</i> , <i>weight3</i> , and <i>weight4</i> specify the ratio of the frequency in which the SRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 255.
--------------------	--	--

**Defaults** Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among themselves.

If you configure a shaped queue weight to 0 by using the **srr-queue bandwidth shape** interface configuration command, this queue participates in SRR shared mode. The weight specified with the **srr-queue bandwidth shape** command is ignored, and the weights specified with the **srr-queue bandwidth share** interface configuration command for a queue take effect.

When configuring queues for the same port for both shaping and sharing, make sure that you configure the lowest numbered queue for shaping.



**Note** The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

## Examples

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used. The bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet0/1
```

**srr-queue bandwidth share**

```
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface [interface-id] queueing** privileged EXEC command.

Related Commands	Command	Description
	<a href="#">mls qos queue-set output buffers</a>	Allocates buffers to a queue-set.
	<a href="#">mls qos srr-queue output cos-map</a>	Maps class of service (CoS) values to an egress queue or maps CoS values to a queue and to a threshold ID.
	<a href="#">mls qos srr-queue output dscp-map</a>	Maps Differentiated Services Code Point (DSCP) values to an egress queue or maps DSCP values to a queue and to a threshold ID.
	<a href="#">mls qos queue-set output threshold</a>	Configures the weighted tail-drop (WTD) thresholds, guarantees the availability of buffers, and configures the maximum memory allocation to a queue-set.
	<a href="#">priority-queue</a>	Enables the egress expedite queue on a port.
	<a href="#">queue-set</a>	Maps a port to a queue-set.
	<a href="#">show mls qos interface queueing</a>	Displays quality of service (QoS) information.
	<a href="#">srr-queue bandwidth shape</a>	Assigns the shaped weights and enables bandwidth shaping on the four egress queues mapped to a port.

## storm-control

Use the **storm-control** interface configuration command to enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface. Use the **no** form of this command to return to the default setting.

```
storm-control { {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]} } | {action {shutdown | trap}}
```

```
no storm-control { {broadcast | multicast | unicast} level} | {action {shutdown | trap}}
```

Syntax Description	
<b>broadcast</b>	Enable broadcast storm control on the interface.
<b>multicast</b>	Enable multicast storm control on the interface.
<b>unicast</b>	Enable unicast storm control on the interface.
<b>level <i>level</i> [<i>level-low</i>]</b>	<p>Specify the rising and falling suppression levels as a percentage of total bandwidth of the port.</p> <ul style="list-style-type: none"> <li>• <i>level</i>—Rising suppression level, up to two decimal places. The range is 0.00 to 100.00. Block the flooding of storm packets when the value specified for <i>level</i> is reached.</li> <li>• <i>level-low</i>—(Optional) Falling suppression level, up to two decimal places. The range is 0.00 to 100.00. This value must be less than or equal to the rising suppression value. If you do not configure a falling suppression level, it is set to the rising suppression level.</li> </ul>
<b>level bps <i>bps</i> [<i>bps-low</i>]</b>	<p>Specify the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.</p> <ul style="list-style-type: none"> <li>• <i>bps</i>—Rising suppression level, up to 1 decimal place. The range is 0.0 to 1000000000.0. Block the flooding of storm packets when the value specified for <i>bps</i> is reached.</li> <li>• <i>bps-low</i>—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 1000000000.0. This value must be equal to or less than the rising suppression value.</li> </ul> <p>You can use metric suffixes such as k, m, and g for large number thresholds.</p>
<b>level pps <i>pps</i> [<i>pps-low</i>]</b>	<p>Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.</p> <ul style="list-style-type: none"> <li>• <i>pps</i>—Rising suppression level, up to 1 decimal place. The range is 0.0 to 1000000000.0. Block the flooding of storm packets when the value specified for <i>pps</i> is reached.</li> <li>• <i>pps-low</i>—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 1000000000.0. This value must be equal to or less than the rising suppression value.</li> </ul> <p>You can use metric suffixes such as k, m, and g for large number thresholds.</p>

---

<b>action {shutdown   trap}</b>	Action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>shutdown</b>—Disables the port during a storm.</li><li>• <b>trap</b>—Sends an SNMP trap when a storm occurs.</li></ul>
---------------------------------	---

---

**Defaults**

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

**Command Modes**

Interface configuration

**Command History****Usage Guidelines**

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.



**Note** When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.



**Note** Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

For more information, see the software configuration guide for this release.

**Examples**

This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

```
Switch(config-if)# storm-control broadcast level 75.5
```

This example shows how to enable unicast storm control on a port with a 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if)# storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">show storm-control</a>	Displays broadcast, multicast, or unicast storm control settings on all interfaces or on a specified interface.

**switchport access**

# switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access or dynamic-access port. If the switchport mode is set to **access**, the port operates as a member of the specified VLAN. If set to **dynamic**, the port starts discovery of VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

**switchport access vlan {vlan-id | dynamic}**

**no switchport access vlan**

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094. <b>vlan dynamic</b> Specify that the access mode VLAN is dependent on the VLAN Membership Policy Server (VMPS) protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to get the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.
---------------------------	--

**Defaults**

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

**Command Modes**

Interface configuration

**Command History****Usage Guidelines**

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

The port must be in access mode before the **switchport access vlan** command can take effect.

An access port can be assigned to only one VLAN.

The VMPS server (such as a Catalyst 6000 series switch) must be configured before a port is configured as dynamic.

These restrictions apply to dynamic-access ports:

- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6000 series switch. The Catalyst switches are not VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.

- Configure the network so that STP does not put the dynamic-access port into an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as
  - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
  - Source or destination ports in a static address entry.
  - Monitor ports.

**Examples**

This example shows how to change a switched port interface that is operating in access mode to operate in VLAN 2 instead of the default VLAN:

```
Switch(config-if)# switchport access vlan 2
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
<b>switchport mode</b>	Configures the VLAN membership mode of a port.

---

switchport backup interface

# switchport backup interface

Use the **switchport backup interface** interface configuration command on a Layer 2 interface to configure Flex Links, a pair of interfaces that provide backup to each other. Use the **no** form of this command to remove the Flex Links configuration.

```
switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id | Port-channel interface-id | TenGigabitEthernet interface-id] {mmu primary vlan interface-id | multicast fast-convergence | preemption {delay delay-time | mode} | prefer vlan vlan-id}

no switchport backup interface [FastEthernet interface-id | GigabitEthernet interface-id | Port-channel interface-id | TenGigabitEthernet interface-id] {mmu primary vlan interface-id | multicast fast-convergence | preemption {delay delay-time | mode} | prefer vlan vlan-id}
```

Syntax Description	
<b>FastEthernet</b>	FastEthernet IEEE 802.3 port name. Valid range is 0 to 9.
<b>GigabitEthernet</b>	GigabitEthernet IEEE 802.3z port name. Valid range is 0 to 9.
<b>Port-channel</b>	Ethernet Channel of interface. Valid range is 0 to 48.
<b>TenGigabitEthernet</b>	Ten Gigabit Ethernet port name. Valid range is 0 to 9.
<i>interface-id</i>	Specify that the Layer 2 interface to act as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1 to 48.
<b>mmu</b>	MAC-address move update. Configure the MAC move update (MMU) for a backup interface pair.
<b>primary vlan <i>vlan-id</i></b>	The VLAN ID of the private-VLAN primary VLAN; valid range is 1 to 4,094.
<b>multicast fast-convergence</b>	Multicast Fast-convergence parameter.
<b>preemption</b>	Configure a preemption scheme for a backup interface pair.
<b>delay <i>delay-time</i></b>	(Optional) Specify a preemption delay; the valid values are 1 to 300 seconds.
<b>mode</b>	Specify a preemption mode as bandwidth, forced, or off.
<b>prefer vlan <i>vlan-id</i></b>	Specify that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4,094.
<b>off</b>	(Optional) Specify that no preemption occurs from backup to active.
<b>delay <i>delay-time</i></b>	(Optional) Specify a preemption delay; the valid values are 1 to 300 seconds.

---

## Defaults

The default is to have no Flex Links defined. Preemption mode is off. No preemption occurs. Preemption delay is set to 35 seconds.

---

## Command Modes

Interface configuration

Command History	Release	Modification
	12.2(25)SEE	Added <b>preemption</b> , <b>mode</b> , <b>forced</b> , <b>bandwidth</b> , <b>off</b> , and <b>delay</b> keywords.
	12.2(37)SE	Added <b>prefer</b> <b>vlan</b> keyword.
	12.2(44)SE	The <b>multicast</b> , <b>fast-convergence</b> , <b>delay</b> , <b>mode</b> , <b>prefer</b> , and <b>vlan</b> keywords were added.

**Usage Guidelines**

With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

- This command is available only for Layer 2 interfaces.
- You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.
- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- A backup link does not have to be the same type (Fast Ethernet or Gigabit Ethernet, for instance) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- If STP is configured on the switch, Flex Links do not participate in STP in all valid VLANs. If STP is not running, be sure that there are no loops in the configured topology.

**Examples**

This example shows how to configure two interfaces as Flex Links:

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
```

This example shows how to configure the Fast Ethernet interface to always preempt the backup:

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preemption forced
Switch(conf-if)# end
```

This example shows how to configure the Fast Ethernet interface preemption delay time:

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preemption delay 150
Switch(conf-if)# end
```

This example shows how to configure the Fast Ethernet interface as the MMU primary VLAN:

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
```

**switchport backup interface**

```
Switch(conf-if)# switchport backup interface fastethernet0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

You can verify your setting by entering the **show interfaces switchport backup** privileged EXEC command.

The following example shows how to configure preferred VLANs:

```
Switch(config)# interface gigabitethernet 0/6
Switch(config-if)# switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120
```

You can verify your setting by entering the **show interfaces switchport backup** privileged EXEC command.

In the following example, VLANs 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gi0/6 forwards traffic for VLANs 1 to 50, and Gi0/8 forwards traffic for VLANs 60 and 100 to 120.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface goes down (LINK\_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Down/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
GigabitEthernet0/6	GigabitEthernet0/8	Active Up/Backup Up

```
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

This example shows how to configure multicast fast-convergence on interface Gi0/11:

```
Switch# configure terminal
```

```
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 0/12 multicast
fast-convergence
Switch(config-if)# end
```

You can verify your setting by entering the **show interfaces switchport backup detail** privileged EXEC command.

```
Switch# show interfaces switchport backup detail
```

Switch Backup Interface Pairs:

Active Interface	Backup Interface	State
GigabitEthernet0/11	GigabitEthernet0/12	Active Up/Backup Standby
Preemption Mode : off		
Multicast Fast Convergence : On		
Bandwidth : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)		
Mac Address Move Update Vlan : auto		

#### Related Commands

Command	Description
<a href="#">show interfaces [interface-id]</a>	Displays the configured Flex Links and their status on the switch or for the specified interface.

**switchport block**

# switchport block

Use the **switchport block** interface configuration command to prevent unknown multicast or unicast packets from being forwarded. Use the **no** form of this command to allow forwarding unknown multicast or unicast packets.

**switchport block {multicast | unicast}**

**no switchport block {multicast | unicast}**

<b>Syntax Description</b>	<b>multicast</b>	Specify that unknown multicast traffic should be blocked.  <b>Note</b> Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
	<b>unicast</b>	Specify that unknown unicast traffic should be blocked.

**Defaults** Unknown multicast and unicast traffic is not blocked.

**Command Modes** Interface configuration

**Command History****Usage Guidelines**

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

For more information about blocking packets, see the software configuration guide for this release.

**Examples**

This example shows how to block unknown unicast traffic on an interface:

```
Switch(config-if)# switchport block unicast
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Commands	Command	Description
	<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.

**switchport host**

# switchport host

Use the **switchport host** interface configuration command to optimize a port for a host connection. The **no** form of this command has no affect on the system.

## **switchport host**

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

**Defaults** The default is for the port to not be optimized for a host connection.

**Command Modes** Interface configuration

## **Command History**

**Usage Guidelines** To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

---

## **Examples**

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#

```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

---

## **Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show interfaces switchport</b></a>	Displays the administrative and operational status of a switching port, including switchport mode.

# switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

**switchport mode {access | dynamic {auto | desirable} | trunk}**

**no switchport mode {access | dynamic | trunk}**

Syntax Description	access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the <b>switchport access vlan</b> interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
	<b>dynamic auto</b>	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
	<b>dynamic desirable</b>	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
	<b>trunk</b>	Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

**Defaults** The default mode is **dynamic auto**.

**Command Modes** Interface configuration

## Command History

**Usage Guidelines** A configuration that uses the **access** or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

**switchport mode**

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Access ports trunk ports are mutually exclusive.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

**Examples**

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show interfaces switchport</b></a>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
<a href="#"><b>switchport access</b></a>	Configures a port as a static-access or dynamic-access port.
<a href="#"><b>switchport trunk</b></a>	Configures the trunk characteristics when an interface is in trunking mode.

# switchport nonegotiate

Use the **switchport nonegotiate** interface configuration command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface. The switch does not engage in DTP negotiation on this interface. Use the **no** form of this command to return to the default setting.

**switchport nonegotiate**

**no switchport nonegotiate**

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

**Defaults** The default is to use DTP negotiation to learn the trunking status.

**Command Modes** Interface configuration

## Command History

**Usage Guidelines** The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in **dynamic (auto or desirable)** mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this, you should turn off DTP by using the **switchport no negotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

**switchport nonegotiate****Examples**

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport nonegotiate
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show interfaces switchport</b></a>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
<a href="#"><b>switchport mode</b></a>	Configures the VLAN membership mode of a port.

# switchport port-security

Use the **switchport port-security** interface configuration command without keywords to enable port security on the interface. Use the keywords to configure secure MAC addresses, sticky MAC address learning, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

```
switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}]] |
mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]] [maximum value [vlan
{vlan-list | {access | voice}}]]]
```

```
no switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}]] |
mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]] [maximum value [vlan
{vlan-list | {access | voice}}]]]
```

```
switchport port-security [aging] [violation {protect | restrict | shutdown | shutdown vlan}]
```

```
no switchport port-security [aging] [violation {protect | restrict | shutdown | shutdown vlan}]
```

Syntax Description	
<b>aging</b>	(Optional) See the <a href="#">switchport port-security aging</a> command.
<b>mac-address mac-address</b>	(Optional) Specify a secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
<b>vlan vlan-id</b>	(Optional) On a trunk port only, specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
<b>vlan access</b>	(Optional) On an access port only, specify the VLAN as an access VLAN.
<b>vlan voice</b>	(Optional) On an access port only, specify the VLAN as a voice VLAN.  <b>Note</b> The <b>voice</b> keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
<b>mac-address sticky [mac-address]</b>	(Optional) Enable the interface for <i>sticky learning</i> by entering only the <b>mac-address sticky</b> keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.  (Optional) Enter a <i>mac-address</i> to specify a sticky secure MAC address.
<b>maximum value</b>	(Optional) Set the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.  The default setting is 1.

**switchport port-security**


---

<b>vlan [vlan-list]</b>	(Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the <b>vlan</b> keyword is not entered, the default value is used. <ul style="list-style-type: none"> <li>• <b>vlan</b>—set a per-VLAN maximum value.</li> <li>• <b>vlan vlan-list</b>—set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.</li> </ul>
<b>violation</b>	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is <b>shutdown</b> .
<b>protect</b>	Set the security violation protect mode. In this mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. <p><b>Note</b> We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.</p>
<b>restrict</b>	Set the security violation restrict mode. In this mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
<b>shutdown</b>	Set the security violation shutdown mode. In this mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the <b>errdisable recovery cause psecure-violation</b> global configuration command, or you can manually re-enable it by entering the <b>shutdown</b> and <b>no shut down</b> interface configuration commands.
<b>shutdown vlan</b>	Set the security violation mode to per-VLAN shutdown. In this mode, only the VLAN on which the violation occurred is error-disabled.

---

**Defaults**

The default is to disable port security.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

The default violation mode is **shutdown**.

Sticky learning is disabled.

**Command Modes**

Interface configuration

Command History	Release	Modification
	12.2(35)SE	The <b>shutdown vlan</b> keyword was added

**Usage Guidelines**

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- Voice VLAN is supported only on access ports and not on trunk ports.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command. You can manually re-enable the port by entering the **shutdown** and **no shut down** interface configuration commands or by using the **clear errdisable interface** privileged EXEC command.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

**switchport port-security**

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky *mac-address*** interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky *mac-address*** interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

**Examples**

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

This example shows how to configure a port to shut down only the VLAN if a violation occurs:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config)# switchport port-security violation shutdown vlan
```

You can verify your settings by using the **show port-security** privileged EXEC command.

Related Commands	Command	Description
	<b>clear port-security</b>	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
	<b>show port-security address</b>	Displays all the secure addresses configured on the switch.
	<b>show port-security</b> <b>interface</b> <i>interface-id</i>	Displays port security configuration for the switch or for the specified interface.

**switchport port-security aging**

# switchport port-security aging

Use the **switchport port-security aging** interface configuration command to set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

**switchport port-security aging {static | time *time* | type {absolute | inactivity}}**

**no switchport port-security aging {static | time | type}**

<b>Syntax Description</b>	
<b>static</b>	Enable aging for statically configured secure addresses on this port.
<b>time <i>time</i></b>	Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
<b>type</b>	Set the aging type.
<b>absolute</b>	Set absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
<b>inactivity</b>	Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

**Defaults**

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

**Command Modes**

Interface configuration

**Command History****Usage Guidelines**

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it becomes inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

**Examples**

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

#### Related Commands

Command	Description
<a href="#">show port-security</a>	Displays the port security settings defined for the port.
<a href="#">switchport port-security</a>	Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses.

**switchport priority extend**

# switchport priority extend

Use the **switchport priority extend** interface configuration command to set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port. Use the **no** form of this command to return to the default setting.

**switchport priority extend {cos value | trust}**

**no switchport priority extend**

<b>Syntax Description</b>	<b>cos value</b> Set the IP phone port to override the IEEE 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0. <b>trust</b> Set the IP phone port to trust the IEEE 802.1p priority received from the PC or the attached device.
---------------------------	---

**Defaults** The default port priority is set to a CoS value of 0 for untagged frames received on the port.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

When voice VLAN is enabled, you can configure the switch to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the switch port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all switch interfaces.)

You should configure voice VLAN on switch access ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

### Examples

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport priority extend trust
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

### Related Commands

Command	Description
<b>show interfaces</b>	Displays the administrative and operational status of a switching port.
<b>switchport voice vlan</b>	Configures the voice VLAN on the port.

**switchport protected**

# switchport protected

Use the **switchport protected** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

**switchport protected**

**no switchport protected**

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

**Defaults** No protected port is defined. All ports are nonprotected.

**Command Modes** Interface configuration

## Command History

### Usage Guidelines

The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches. A protected port is different from a secure port.

A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

---

### Examples

This example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport protected
```

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

Syntax Description	Command	Description
	<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
	<b>switchport block</b>	Prevents unknown multicast or unicast traffic on the interface.

# switchport trunk

Use the **switchport trunk** interface configuration command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

**switchport trunk {allowed vlan *vlan-list* | native vlan *vlan-id* | pruning vlan *vlan-list*}**

**no switchport trunk {allowed vlan | native vlan | {pruning vlan}}**

<b>Syntax Description</b>	<b>allowed vlan <i>vlan-list</i></b>	Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following <i>vlan-list</i> format. The <b>none</b> keyword is not valid. The default is <b>all</b> .
	<b>native vlan <i>vlan-id</i></b>	Set the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
	<b>pruning vlan <i>vlan-list</i></b>	Set the list of VLANs that are eligible for VTP pruning when in trunking mode. The <b>all</b> keyword is not valid.

The *vlan-list* format is **all | none | [add | remove | except] *vlan-atom* [,*vlan-atom*...]** where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.



**Note** You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.



**Note** You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **vlan-atom** is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

## Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

---

**Command Modes** Interface configuration

**Command History**
**Usage Guidelines**

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.
- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

---

**Examples**

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings by entering the **show interfaces interface-id switchport** privileged EXEC command.

**switchport trunk**

Related Commands	Command	Description
	<b>show interfaces switchport</b>	Displays the administrative and operational status of a switching port, including port blocking and port protection settings.
	<b>switchport mode</b>	Configures the VLAN membership mode of a port.

# switchport voice vlan

Use the **switchport voice vlan** interface configuration command to configure voice VLAN on the port. Use the **no** form of this command to return to the default setting.

**switchport voice vlan {vlan-id | dot1p | none | untagged}**

**no switchport voice vlan**

<b>Syntax Description</b>	
<b>vlan-id</b>	Specify the VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
<b>dot1p</b>	Configure the switch to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5 and drops all voice and data traffic tagged with VLAN 0.
<b>none</b>	Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
<b>untagged</b>	Configure the telephone to send untagged voice traffic. This is the default for the telephone.

## Defaults

The switch default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames. The switch drops all traffic tagged with VLAN ID 0.

## Command Modes

Interface configuration

## Command History

### Usage Guidelines

You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switchport connected to the Cisco IP phone for the switch to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the switch by entering the **mls qos** global configuration command and configure the port trust state to trust by entering the **mls qos trust cos** interface configuration command.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The switch puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select **dot1q**, **none**, or **untagged**, the switch puts the indicated voice traffic in the access VLAN.

When you enter the **switchport voice vlan dot1q** command, the switch can receive 802.1Q priority voice and data traffic tagged with VLAN 0.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

**switchport voice vlan**

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

**Examples**

This example shows how to configure VLAN 2 as the voice VLAN for the port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport voice vlan 2
```

You can verify your settings by entering the **show interfaces *interface-id* switchport** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show interfaces <i>interface-id</i> switchport</b>	Displays the administrative and operational status of a switching port.
<b>switchport priority extend</b>	Decides how the device connected to the specified port handles priority traffic received on its incoming port.

# system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for Gigabit Ethernet ports or for Fast Ethernet (10/100) ports. Use the **no** form of this command to restore the global MTU value to its default value.

**system mtu {bytes | jumbo bytes}**

**no system mtu**

Syntax Description	bytes	Set the system MTU for ports that are set to 10 or 100 Mb/s. The range is 1500 to 1998 bytes. This is the maximum MTU received at 10/100-Mb/s Ethernet switch ports.
	jumbo bytes	Set the system jumbo MTU for Gigabit Ethernet ports operating at 1000 Mb/s or greater. The range is 1500 to 9000 bytes. This is the maximum MTU received at the physical port for Gigabit Ethernet ports.

## Defaults

The default MTU size for all ports is 1500 bytes.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

When you use this command to change the system MTU or jumbo MTU size, you must reset the switch before the new configuration takes effect. The system MTU setting is saved in the switch environmental variable in NVRAM and becomes effective when the switch reloads. The MTU settings you enter with the **system mtu** and **system mtu jumbo** commands are not saved in the switch IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu** and **system mtu jumbo** settings on the new switch and then reload the switch.

Gigabit Ethernet ports operating at 1000 Mb/s are not affected by the **system mtu** command, and 10/100-Mb/s ports are not affected by the **system mtu jumbo** command.

If you enter a value that is outside the range for the specific type of switch, the value is not accepted.



### Note

The switch does not support setting the MTU on a per-interface basis.

The size of frames that can be received by the switch CPU is limited to 1998 bytes, regardless of the value entered with the **system mtu** command. Although forwarded or routed frames are usually not received by the CPU, some packets (for example, control traffic, SNMP, Telnet, and routing protocols) are sent to the CPU.

**system mtu**

For example, if the **system mtu** value is 1998 bytes and the **system mtu jumbo** value is 5000 bytes, packets up to 5000 bytes can be received on interfaces operating at 1000 Mb/s. However, although a packet larger than 1998 bytes can be received on an interface operating at 1000 Mb/s, if its destination interface is operating at 10 or 100 Mb/s, the packet is dropped.

**Examples**

This example shows how to set the maximum jumbo packet size for Gigabit Ethernet ports operating at 1000 Mb/s or greater to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

You can verify your setting by entering the **show system mtu** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show system mtu</a>	

# test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** privileged EXEC command to run the Time Domain Reflector (TDR) feature on an interface.

**test cable-diagnostics tdr interface *interface-id***

<b>Syntax Description</b>	<i>interface-id</i>	Specify the interface on which to run TDR.
---------------------------	---------------------	--

<b>Defaults</b>	There is no default.
-----------------	----------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

**Usage Guidelines** For more information about TDR, see the software configuration guide for this release.

After you run TDR by using the **test cable-diagnostics tdr interface *interface-id*** command, use the **show cable-diagnostics tdr interface *interface-id*** privileged EXEC command to display the results.

<b>Examples</b>	This example shows how to run TDR on an interface:
-----------------	--

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

If you enter the **test cable-diagnostics tdr interface *interface-id*** command on an interface that has a link status of up and a speed of 10 or 100 Mb/s, these messages appear:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/3 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show cable-diagnostics tdr</a>	Displays the TDR results.

traceroute mac

## traceroute mac

Use the **traceroute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

```
traceroute mac [interface interface-id] {source-mac-address} [interface interface-id]
{destination-mac-address} [vlan vlan-id] [detail]
```

Syntax Description	
<b>interface interface-id</b>	(Optional) Specify an interface on the source or destination switch.
<b>source-mac-address</b>	Specify the MAC address of the source switch in hexadecimal format.
<b>destination-mac-address</b>	Specify the MAC address of the destination switch in hexadecimal format.
<b>vlan vlan-id</b>	(Optional) Specify the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. Valid VLAN IDs are 1 to 4094.
<b>detail</b>	(Optional) Specify that detailed information appears.

### Defaults

There is no default.

### Command Modes

Privileged EXEC

### Command History

#### Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

**Examples**

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[switch_mmodel] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5 (2.2.5.5) : Gi0/3 => Gi0/1
con1 (2.2.1.1) : Gi0/1 => Gi0/2
con2 (2.2.2.2) : Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[switch_mmodel] (2.2.6.6)
con6 /switch_mmodel/ 2.2.6.6 :
    Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / switch_mmodel / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 /switch_mmodel / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[switch_mmodel] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5 (2.2.5.5) : Gi0/3 => Gi0/1
con1 (2.2.1.1) : Gi0/1 => G0/2
con2 (2.2.2.2) : Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[switch_mmodel] (2.2.5.5)
con5 / switch_mmodel / 2.2.5.5 :
    Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / switch_mmodel / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
```

**traceroute mac**

Error:Source and destination macs are on different vlans.  
Layer2 trace aborted.

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>traceroute mac ip</b></a>	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

# traceroute mac ip

Use the **traceroute mac ip** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

```
traceroute mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]
```

Syntax Description		
<i>source-ip-address</i>	Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format.	
<i>destination-ip-address</i>	Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.	
<i>source-hostname</i>	Specify the IP hostname of the source switch.	
<i>destination-hostname</i>	Specify the IP hostname of the destination switch.	
<b>detail</b>	(Optional) Specify that detailed information appears.	

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

### Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

**traceroute mac ip****Examples**

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / switch_mmodel / 2.2.6.6 :
    Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / switch_mmodel / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / switch_mmodel / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / switch_mmodel / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5          (2.2.5.5      ) : Gi0/3 => Gi0/1
con1          (2.2.1.1      ) : Gi0/1 => Gi0/2
con2          (2.2.2.2      ) : Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>traceroute mac</b></a>	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

## trust

Use the **trust** policy-map class configuration command to define a trust state for traffic classified through the **class** policy-map configuration or the **class-map** global configuration command. Use the **no** form of this command to return to the default setting.

```
trust [cos | dscp | ip-precedence]
no trust [cos | dscp | ip-precedence]
```

Syntax Description	
<b>cos</b>	(Optional) Classify an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used.
<b>dscp</b>	(Optional) Classify an ingress packet by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP.
<b>ip-precedence</b>	(Optional) Classify an ingress packet by using the packet IP-precedence value (most significant 3 bits of 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the port default CoS value is used to map CoS to DSCP.

**Defaults** The action is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

**Command Modes** Policy-map class configuration

### Command History

### Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, incoming traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the incoming traffic.

Trust values set with this command supersede trust values set with the **mls qos trust** interface configuration command.

The **trust** command is mutually exclusive with **set** policy-map class configuration command within the same policy map.

If you specify **trust cos**, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify **trust dscp**, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS uses the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP for the packet is derived from the CoS-to-DSCP map.

**trust**

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

**Examples**

This example shows how to define a port trust state to trust incoming DSCP values for traffic classified with *class1*:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>class</b></a>	Defines a traffic classification match criteria (through the <b>police</b> , <b>set</b> , and <b>trust</b> policy-map class configuration commands) for the specified class-map name.
<a href="#"><b>police</b></a>	Defines a policer for classified traffic.
<a href="#"><b>policy-map</b></a>	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
<a href="#"><b>set</b></a>	Classifies IP traffic by setting a DSCP or IP-precedence value in the packet.
<a href="#"><b>show policy-map</b></a>	Displays QoS policy maps.

# udld

Use the **udld** global configuration command to enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time. Use the **no** form of the command to disable aggressive or normal mode UDLD on all fiber-optic ports.

**udld {aggressive | enable | message time *message-timer-interval*}**

**no udld {aggressive | enable | message}**

Syntax Description	<b>aggressive</b> Enable UDLD in aggressive mode on all fiber-optic interfaces. <b>enable</b> Enable UDLD in normal mode on all fiber-optic interfaces. <b>message time</b> Configure the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is to 90 seconds. <i>message-timer-interval</i>
--------------------	--

## Defaults

UDLD is disabled on all interfaces.

The message timer is set at 15 seconds.

## Command Modes

Global configuration

## Command History

### Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Understanding UDLD” section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to re-enable UDLD globally
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval *interval*** global configuration commands to automatically recover from the UDLD error-disabled state

**Examples**

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show udld</b></a>	Displays UDLD administrative and operational status for all ports or the specified port.
<a href="#"><b>udld port</b></a>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.
<a href="#"><b>udld reset</b></a>	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

# udld port

Use the **udld port** interface configuration command to enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic interface from being enabled by the **udld** global configuration command. Use the **no** form of this command to return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port.

**udld port [aggressive]**

**no udld port [aggressive]**

<b>Syntax Description</b>	<b>aggressive</b>	Enable UDLD in aggressive mode on the specified interface.
---------------------------	-------------------	--

## Defaults

On fiber-optic interfaces, UDLD is not enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

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

## Command History

### Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to re-enable UDLD globally

**udld port**

- The **no udld port** interface configuration command followed by the **udld port or udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval interval** global configuration commands to automatically recover from the UDLD error-disabled state

**Examples**

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show running-config</b>	Displays the running configuration on the switch.
<b>show udld</b>	Displays UDLD administrative and operational status for all ports or the specified port.
<b>udld</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
<b>udld reset</b>	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

# udld reset

Use the **udld reset** privileged EXEC command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled).

## udld reset

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

**Command Modes** Privileged EXEC

### Command History

**Usage Guidelines** If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

**Examples** This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

You can verify your setting by entering the **show udld** privileged EXEC command.

Related Commands	Command	Description
	<b>show running-config</b>	Displays the running configuration on the switch.
	<b>show udld</b>	Displays UDLD administrative and operational status for all ports or the specified port.
	<b>udld</b>	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
	<b>udld port</b>	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the <b>udld</b> global configuration command.

# vlan

Use the **vlan** global configuration command to add a VLAN and to enter the config-vlan mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database. When VLAN Trunking Protocol (VTP) mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005), and the VTP mode, domain name, and the VLAN configuration are saved in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

**vlan *vlan-id***

**no vlan *vlan-id***

<b>Syntax Description</b>	<i>vlan-id</i>	ID of the VLAN to be added and configured. For <i>vlan-id</i> , the range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.
---------------------------	----------------	--

**Defaults** This command has no default settings.

**Command Modes** Global configuration

## Command History

### Usage Guidelines

You must use the **vlan *vlan-id*** global configuration command to add extended-range VLANs (VLAN IDs 1006 to 4094). Before configuring VLANs in the extended range, you must use the **vtp transparent** global configuration or VLAN configuration command to put the switch in VTP transparent mode. Extended-range VLANs are not learned by VTP and are not added to the VLAN database, but when VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is selected in these ways:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode is server, or if the startup VTP mode or domain names do not match the VLAN database, the VTP mode and the VLAN configuration for the first 1005 VLANs use the VLAN database information.

If you try to create an extended-range VLAN when the switch is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

If you enter an invalid VLAN ID, you receive an error message and do not enter config-vlan mode.

Entering the **vlan** command with a VLAN ID enables config-vlan mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the config-vlan mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in config-vlan mode. The **no** form of each command returns the characteristic to its default state.


**Note**


---

Although all commands are visible, the only VLAN configuration commands that are supported on extended-range VLANs are **mtu mtu-size** and **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

---

- **are are-number:** defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf:** specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable** backup CRF mode for this VLAN.
  - **disable** backup CRF mode for this VLAN (the default).
- **bridge {bridge-number| type}:** specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
  - **srbb** (source-route bridging)
  - **srt** (source-route transparent) bridging VLAN
- **exit:** applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits config-vlan mode.
- **media:** defines the VLAN media type. See [Table 1-1](#) for valid commands and syntax for different media types.


**Note**


---

The switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

---

- **ethernet** is Ethernet media type (the default).
- **fddi** is FDDI media type.
- **fd-net** is FDDI network entity title (NET) media type.
- **tokenring** is Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
- **tr-net** is Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.
- **mtu mtu-size:** specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.
- **name vlan-name:** names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.

- **no:** negates a command or returns it to the default setting.
- **parent parent-vlan-id:** specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.
- **remote-span:** configure the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN-IDs that are lower than 1024. Learning is disabled on the VLAN. See the **remote-span** command for more information.
- **ring ring-number:** defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said said-value:** specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown:** shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit config-vlan mode.
- **state:** specifies the VLAN state:
  - **active** means the VLAN is operational (the default).
  - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste ste-number:** defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type:** defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is **ieee**. For Token Ring-NET VLANs, the default STP type is **ibm**. For FDDI and Token Ring VLANs, the default is no type specified.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).
  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1 tb-vlan1-id** and **tb-vlan2 tb-vlan2-id:** specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

**Table 1-1** Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	<b>name vlan-name, media ethernet, state {suspend   active}, said said-value, mtu mtu-size, remote-span, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b>
FDDI	<b>name vlan-name, media fddi, state {suspend   active}, said said-value, mtu mtu-size, ring ring-number, parent parent-vlan-id, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b>

**Table 1-1** Valid Commands and Syntax for Different Media Types (continued)

Media Type	Valid Syntax
FDDI-NET	<b>name vlan-name, media fd-net, state {suspend   active}, said said-value, mtu mtu-size, bridge bridge-number, stp type {ieee   ibm   auto}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b> If VTP v2 mode is disabled, do not set the <b>stp type</b> to <b>auto</b> .
Token Ring	VTP v1 mode is enabled. <b>name vlan-name, media tokenring, state {suspend   active}, said said-value, mtu mtu-size, ring ring-number, parent parent-vlan-id, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b>
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. <b>name vlan-name, media tokenring, state {suspend   active}, said said-value, mtu mtu-size, ring ring-number, parent parent-vlan-id, bridge type {srp   srt}, are are-number, ste ste-number, backupcrf {enable   disable}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b>
Token Ring-NET	VTP v1 mode is enabled. <b>name vlan-name, media tr-net, state {suspend   active}, said said-value, mtu mtu-size, bridge bridge-number, stp type {ieee   ibm}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b>
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. <b>name vlan-name, media tr-net, state {suspend   active}, said said-value, mtu mtu-size, bridge bridge-number, stp type {ieee   ibm   auto}, tb-vlan1 tb-vlan1-id, tb-vlan2 tb-vlan2-id</b>

Table 1-2 describes the rules for configuring VLANs.

**Table 1-2** VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.

**Table 1-2 VLAN Configuration Rules (continued)**

Configuration	Rule
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

**Examples**

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** config-vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter config-vlan mode, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

**Related Commands**

Command	Description
<b>show vlan</b>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

# vmpls reconfirm (privileged EXEC)

Use the **vmpls reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

## vmpls reconfirm

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

**Defaults** No default is defined.

**Command Modes** Privileged EXEC

## Command History

**Examples** This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmpls reconfirm
```

You can verify your setting by entering the **show vmpls** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmpls** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmpls reconfirm** command was entered.

## Related Commands

Command	Description
<a href="#">show vmpls</a>	Displays VQP and VMPS information.
<a href="#">vmpls reconfirm (global configuration)</a>	Changes the reconfirmation interval for the VQP client.

---

 vmps reconfirm (global configuration)
 

---

# vmps reconfirm (global configuration)

Use the **vmps reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmps reconfirm** *interval*

**no vmps reconfirm**

---

<b>Syntax Description</b>	<i>interval</i>	Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes.
---------------------------	-----------------	--

---

**Defaults** The default reconfirmation interval is 60 minutes.

**Command Modes** Global configuration

---

## Command History

### Examples

This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmps reconfirm 20
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Reconfirm Interval row.

---

Related Commands	Command	Description
	<a href="#">show vmps</a>	Displays VQP and VMPS information.
	<a href="#">vmps reconfirm (privileged EXEC)</a>	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.

---

# vmpls retry

Use the **vmpls retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmpls retry count**

**no vmpls retry**

---

<b>Syntax Description</b>	<i>count</i> Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10.
---------------------------	--

---

<b>Defaults</b>	The default retry count is 3.
-----------------	-------------------------------

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

## Command History

<b>Examples</b>	This example shows how to set the retry count to 7:
-----------------	---

```
Switch(config)# vmpls retry 7
```

You can verify your setting by entering the **show vmpls** privileged EXEC command and examining information in the Server Retry Count row.

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show vmpls</a>	Displays VQP and VMPS information.

---

## vmps server

Use the **vmps server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server.

**vmps server** *ipaddress* [**primary**]

**no vmps server** [*ipaddress*]

<b>Syntax Description</b>	<table border="0"> <tr> <td><i>ipaddress</i></td><td>IP address or hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured.</td></tr> <tr> <td><b>primary</b></td><td>(Optional) Decides whether primary or secondary VMPS servers are being configured.</td></tr> </table>	<i>ipaddress</i>	IP address or hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured.	<b>primary</b>	(Optional) Decides whether primary or secondary VMPS servers are being configured.
<i>ipaddress</i>	IP address or hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured.				
<b>primary</b>	(Optional) Decides whether primary or secondary VMPS servers are being configured.				

**Defaults** No primary or secondary VMPS servers are defined.

**Command Modes** Global configuration

### Command History

#### Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. The first server address can be overridden by using **primary** in a subsequent command.

If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.

When using the **no** form without specifying the *ipaddress*, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.

#### Examples

This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmps server 191.10.49.21
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the VMPS Domain Server row.

**Related Commands**

Command	Description
<a href="#">show vmps</a>	Displays VQP and VMPS information.

# vtp (global configuration)

Use the **vtp** global configuration command to set or modify the VLAN Trunking Protocol (VTP) configuration characteristics. Use the **no** form of this command to remove the settings or to return to the default settings.

```
vtp {domain domain-name | file filename | interface name [only] | mode {client | off | server | transparent} [mst | unknown | vlan] | password password [hidden | secret] | pruning | version number}

no vtp {file | interface | mode [client | off | server | transparent] [mst | unknown | vlan] | password | pruning | version}
```

Syntax Description	
<b>domain domain-name</b>	Specify the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
<b>file filename</b>	Specify the Cisco IOS file system file where the VTP VLAN configuration is stored.
<b>interface name</b>	Specify the name of the interface providing the VTP ID updated for this device.
<b>only</b>	(Optional) Use only the IP address of this interface as the VTP IP updater.
<b>mode</b>	Specify the VTP device mode as client, server, or transparent.
<b>client</b>	Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
<b>off</b>	Place the switch in VTP off mode. A switch in off VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
<b>server</b>	Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
<b>transparent</b>	Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.  When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the <b>copy running-config startup config</b> privileged EXEC command.
<b>mst</b>	(Optional) Set the mode for the multiple spanning tree (MST) VTP database (only VTP version 3).
<b>unknown</b>	(Optional) Set the mode for unknown VTP databases (only VTP version 3).

<b>vlan</b>	(Optional) Set the mode for VLAN VTP database. This is the default (only VTP version 3).
<b>password password</b>	Set the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
<b>hidden</b>	(Optional) Specify that the key generated from the password string is saved in the VLAN database file. When the <b>hidden</b> keyword is not specified, the password string is saved in clear text. When the <b>hidden</b> password is entered, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP version 3.
<b>secret</b>	(Optional) Allow the user to directly configure the password secret key (only VTP version 3).
<b>pruning</b>	Enable VTP pruning on the switch.
<b>version number</b>	Set VTP version to version 1, version 2, or version 3.

**Defaults**

The default filename is *flash:vlan.dat*.

The default mode is server mode and the default database is VLAN.

In VTP version 3, for the MST database, the default mode is transparent.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

**Command Modes**

Global configuration

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(52)SE	The <b>mode off</b> keyword was added, support was added for VTP version 3, and the password <b>hidden</b> and <b>secret</b> keywords and the mode database keywords ( <b>vlan</b> , <b>mst</b> , and <b>unknown</b> ) were added with VTP version 3.

**Usage Guidelines**

When you save VTP mode, domain name, and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are selected by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are selected by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.

**vtp (global configuration)**

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, it can no be configured to re-enter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- In VTP versions 1 and 2, the VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file. VTP supports extended-range VLANs in client and server mode and saved them in the VLAN database.
- With VTP versions 1 and 2, if extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed. Changing VTP mode is allowed with extended VLANs in VTP version 3.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.
- The **hidden** and **secret** keywords are supported only in VTP version 3. If you convert from VTP version 2 to VTP version 3, you must remove the **hidden** or **secret** keyword before the conversion.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all switches in a domain are VTP Version 2-capable, you need only to configure Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP version 3 regions can only communicate over a VTP version 1 or VTP version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the switch configuration file.

## Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Switch(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

**vtp (global configuration)**

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#"><b>show vtp status</b></a>	Displays the VTP statistics for the switch and general information about the VTP management domain status.
<a href="#"><b>vtp (interface configuration)</b></a>	Enables or disables VTP on an interface.

# vtp (interface configuration)

Use the **vtp** interface configuration command to enable the VLAN Trunking Protocol (VTP) on a per-port basis. Use the **no** form of this command to disable VTP on the interface.

**vtp**

**no vtp**



**Note** This command is supported only when the switch is running the LAN base image and VTP version 3.

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

**Command Default** This command has no default settings.

**Command Modes** Interface configuration.

Command History	Release	Modification
	12.2(52)SE	This command was introduced.

**Usage Guidelines** Enter this command only on interfaces that are switchport in trunk mode.

This command is supported only on switches configured for VTP version 3.

**Examples** This example shows how to enable VTP on an interface:

```
Switch(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Switch(config-if)# no vtp
```

Related Commands	Command	Description
	<a href="#">vtp (global configuration)</a>	Globally configures VTP domain-name, password, pruning, version, and mode.

**vtp primary**

# vtp primary

Use the **vtp primary** privileged EXEC command to configure a switch as the VLAN Trunking Protocol (VTP) primary server.

**vtp primary [mst | vlan] [force]**

There is no **no** form of the command.


**Note**


---

This command is supported only when the switch is running VTP version 3.

---


**Note**


---

Although visible in the command line help, the **vtp {password password | pruning | version number}** commands are not supported.

---



---

**Syntax Description**

<b>mst</b>	(Optional) Configure the switch as the primary VTP server for the multiple spanning tree (MST) feature.
<b>vlan</b>	(Optional) Configure the switch as the primary VTP server for VLANs.
<b>force</b>	(Optional) Configure the switch to not check for conflicting devices when configuring the primary server.

---



---

**Defaults**

The switch is a VTP secondary server.

---

**Command Modes**

Privileged EXEC

---

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(52)SE	This command was introduced.

---



---

**Usage Guidelines**

This command is supported only on switches configured for VTP version 3.

A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.

**Examples**

This example shows how to configure the switch as the primary VTP server for VLANs:

```
Switch# vtp primary vlan  
Setting device to VTP TRANSPARENT mode.
```

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

**Related Commands**

Command	Description
<a href="#">show vtp status</a>	Displays the VTP statistics for the switch and general information about the VTP management domain status.
<a href="#">vtp (global configuration)</a>	Configures the VTP filename, interface, domain name, mode, and version.



## Catalyst Switch Bootloader Commands

During normal bootloader operation, you are not presented with the bootloader command-line prompt. You gain access to the bootloader command line if the switch is set to manually boot up, if an error occurs during power-on self test (POST) DRAM testing, or if an error occurs while loading the operating system (a corrupted Cisco IOS image). You can also access the bootloader if you have lost or forgotten the switch password.

**Note**

The default switch configuration allows an end user with physical access to the switch to recover from a lost password by interrupting the bootup process while the switch is powering up and then entering a new password. The password recovery disable feature allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the bootup process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the bootup process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted. For more information, see the software configuration guide for this release.

You can access the bootloader through a switch console connection at 9600 bps.

Unplug the switch power cord, and press the switch **Mode** button while reconnecting the power cord. You can release the **Mode** button a second or two after the LED above port 1X goes off. You should then see the bootloader *Switch:* prompt. The bootloader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

# boot

Use the **boot** bootloader command to load and boot up an executable image and to enter the command-line interface.

```
boot [-post | -n | -p | flag] filesystem:/file-url ...
```

Syntax Description	-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
	-n	(Optional) Pause for the Cisco IOS debugger immediately after launching.
	-p	(Optional) Pause for the JTAG debugger right after loading the image.
	filesystem:	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
	/file-url	(Optional) Path (directory) and name of a bootable image. Separate image names with a semicolon.

## Defaults

The switch attempts to automatically boot up the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

## Command Modes

Bootloader

## Command History

## Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot up the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot up the specified image.

When you set bootloader **boot** command options, they are executed immediately and apply only to the current bootloader session. These settings are not saved for the next bootup operation.

Filenames and directory names are case sensitive.

## Examples

This example shows how to boot up the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

**boot**

Related Commands	Command	Description
	<b>set</b>	Sets the BOOT environment variable to boot a specific image when the <b>BOOT</b> keyword is appended to the command.

# cat

Use the **cat** bootloader command to display the contents of one or more files.

**cat** *filesystem:/file-url ...*

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a flash file system. Use <b>flash:</b> for the system board flash device. <i>/file-url</i> Path (directory) and name of the files to display. Separate each filename with a space.
---------------------------	--

<b>Command Modes</b>	Bootloader
----------------------	------------

## Command History

**Usage Guidelines** Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

## Examples

This example shows how to display the contents of two files with sample output:

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128LAYER_2|MIN_DRAM_MEG=64
image_family:switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

## Related Commands

Command	Description
<a href="#">more</a>	Displays the contents of one or more files.
<a href="#">type</a>	Displays the contents of one or more files.

**copy**

# copy

Use the **copy** bootloader command to copy a file from a source to a destination.

```
copy [-b block-size] filesystem:/source-file-url filesystem:/destination-file-url
```

**Syntax Description**

<b>-b block-size</b>	(Optional) This option is used only for internal development and testing.
<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/source-file-url</i>	Path (directory) and filename (source) to be copied.
<i>/destination-file-url</i>	Path (directory) and filename of the destination.

**Defaults**

The default block size is 4 KB.

**Command Modes**

Bootloader

**Command History****Usage Guidelines**

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

**Examples**

This example show how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

You can verify that the file was copied by entering the **dir filesystem:** bootloader command.

**Related Commands**

Command	Description
<a href="#">delete</a>	Deletes one or more files from the specified file system.

# delete

Use the **delete** bootloader command to delete one or more files from the specified file system.

**delete** *filesystem:/file-url* ...

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a flash file system. Use <b>flash:</b> for the system board flash device. <i>/file-url</i> Path (directory) and filename to delete. Separate each filename with a space.
---------------------------	--

<b>Command Modes</b>	Bootloader
----------------------	------------

## Command History

**Usage Guidelines** Filenames and directory names are case sensitive.

The switch prompts you for confirmation before deleting each file.

<b>Examples</b>	This example shows how to delete two files:
-----------------	---

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir flash:** bootloader command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">copy</a>	Copies a file from a source to a destination.

dir

# dir

Use the **dir** bootloader command to display a list of files and directories on the specified file system.

**dir** *filesystem:/file-url ...*

## Syntax Description

<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/file-url</i>	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

## Command Modes

Bootloader

## Command History

## Usage Guidelines

Directory names are case sensitive.

## Examples

This example shows how to display the files in flash memory:

```
switch: dir flash:
Directory of flash:/

      3  -rwx        1839  Mar  01 2002 00:48:15  config.text
     11  -rwx       1140  Mar  01 2002 04:18:48  vlan.dat
     21  -rwx        26  Mar  01 2002 00:01:39  env_vars
      9  drwx       768  Mar  01 2002 23:11:42  html
     16  -rwx      1037  Mar  01 2002 00:01:11  config.text
     14  -rwx      1099  Mar  01 2002 01:14:05  homepage.htm
     22  -rwx        96  Mar  01 2002 00:01:39  system_env_vars
     17  drwx       192  Mar  06 2002 23:22:03  imnage-name

15998976 bytes total (6397440 bytes free)
```

Table 1-1 describes the fields in the display.

**Table 1-1** *dir Field Descriptions*

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> <li>• d—directory</li> <li>• r—readable</li> <li>• w—writable</li> <li>• x—executable</li> </ul>
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

**Related Commands**

Command	Description
<a href="#">mkdir</a>	Creates one or more directories.
<a href="#">rmdir</a>	Removes one or more directories.

**flash\_init**

## flash\_init

Use the **flash\_init** bootloader command to initialize the flash file system.

### **flash\_init**

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

**Defaults** The flash file system is automatically initialized during normal system operation.

**Command Modes** Bootloader

### **Command History**

**Usage Guidelines** During the normal bootup process, the flash file system is automatically initialized.

Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

# format

Use the **format** bootloader command to format the specified file system and destroy all data in that file system.

**format** *filesystem:*

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
---------------------------	--

<b>Command Modes</b>	Bootloader
----------------------	------------

---

**Command History****Usage Guidelines**

**Caution** Use this command with care; it destroys all data on the file system and renders your system unusable.

# fsck

Use the **fsck** bootloader command to check the file system for consistency.

**fsck [-test | -f] filesystem:**

Syntax Description	<b>-test</b> (Optional) Initialize the file system code and perform extra POST on flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system. <b>-f</b> (Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked. <b>filesystem:</b> Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
--------------------	---

**Defaults** No file system check is performed.

**Command Modes** Bootloader

## Command History

**Usage Guidelines** To stop an in-progress file system consistency check, disconnect the switch power and then reconnect the power.

**Examples** This example shows how to perform an extensive file system check on flash memory:

```
switch: fsck -test flash:
```

# help

Use the **help** bootloader command to display the available commands.

```
help
```

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

**Command Modes** Bootloader

**Command History**

**Usage Guidelines** You can also use the question mark (?) to display a list of available bootloader commands.

**memory**

# memory

Use the **memory** bootloader command to display memory heap utilization information.

**memory**

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

**Command Modes** Bootloader

**Command History****Examples**

This example shows how to display memory heap utilization information:

```
switch: memory
Text: 0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data: 0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss: 0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Heap: 0x00756f98 - 0x00800000 (0x000a9068 bytes)

Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

Table 1-2 describes the fields in the display.

**Table 1-2** *memory Field Descriptions*

Field	Description
Text	Beginning and ending address of the text storage area.
Rotext	Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry.
Data	Beginning and ending address of the data segment storage area.
Bss	Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.

# mkdir

Use the **mkdir** bootloader command to create one or more new directories on the specified file system.

**mkdir** *filesystem:/directory-url* ...

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a flash file system. Use <b>flash:</b> for the system board flash device. <i>/directory-url</i> Name of the directories to create. Separate each directory name with a space.
---------------------------	---

<b>Command Modes</b>	Bootloader
----------------------	------------

## Command History

### Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

### Examples

This example shows how to make a directory called Saved\_Configs:

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir filesystem:** bootloader command.

### Related Commands

Command	Description
<a href="#">dir</a>	Displays a list of files and directories on the specified file system.
<a href="#">rmdir</a>	Removes one or more directories from the specified file system.

**more**

## more

Use the **more** bootloader command to display the contents of one or more files.

**more** *filesystem:/file-url ...*

<b>Syntax Description</b>	<i>filesystem:</i> Alias for a flash file system. Use <b>flash:</b> for the system board flash device. <i>/file-url</i> Path (directory) and name of the files to display. Separate each filename with a space.
---------------------------	--

<b>Command Modes</b>	Bootloader
----------------------	------------

### Command History

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

<b>Examples</b>	This example shows how to display the contents of two files:
-----------------	--

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name

image_name:image-name.bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cat</b>	Displays the contents of one or more files.
	<b>type</b>	Displays the contents of one or more files.

# rename

Use the **rename** bootloader command to rename a file.

```
rename filesystem:/source-file-url filesystem:/destination-file-url
```

---

## Syntax Description

<i>filesystem:</i>	Alias for a flash file system. Use <b>flash:</b> for the system board flash device.
<i>/source-file-url</i>	Original path (directory) and filename.
<i>/destination-file-url</i>	New path (directory) and filename.

---



---

## Command Modes

Bootloader

---

## Command History

---

### Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

---

## Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
switch: rename flash:config.text flash:config1.text
```

You can verify that the file was renamed by entering the **dir filesystem:** bootloader command.

---

## Related Commands

Command	Description
<a href="#">copy</a>	Copies a file from a source to a destination.

---

**reset**

# reset

Use the **reset** bootloader command to perform a hard reset on the system. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

**reset**

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

**Command Modes** Bootloader

## Command History

### Examples

This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

### Related Commands

Command	Description
<a href="#">boot</a>	Loads and boots up an executable image and enters the command-line interface.

# rmdir

Use the **rmdir** bootloader command to remove one or more empty directories from the specified file system.

**rmdir** *filesystem:/directory-url* ...

<b>Syntax Description</b>	<p><b>filesystem:</b> Alias for a flash file system. Use <b>flash:</b> for the system board flash device.</p> <p><b>/directory-url</b> Path (directory) and name of the empty directories to remove. Separate each directory name with a space.</p>
---------------------------	---

<b>Command Modes</b>	Bootloader
----------------------	------------

## Command History

<b>Usage Guidelines</b>	Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.  Before removing a directory, you must first delete all the files in the directory.  The switch prompts you for confirmation before deleting each directory.
-------------------------	--

<b>Examples</b>	This example shows how to remove a directory:
-----------------	---

```
switch: rmdir flash:Test
```

You can verify that the directory was deleted by entering the **dir filesystem:** bootloader command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dir</b>	Displays a list of files and directories on the specified file system.
	<b>mkdir</b>	Creates one or more new directories on the specified file system.

## set

Use the **set** bootloader command to set or display environment variables, which can be used to control the bootloader or any other software running on the switch.

**set** *variable value*

Syntax Description	<i>variable value</i>	Use one of these keywords for <i>variable and value</i> :
	<b>MANUAL_BOOT</b>	—Decides whether the switch automatically or manually boots up. Valid values are 1, yes, 0, and no. If it is set to no or 0, the bootloader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the bootloader mode.
	<b>BOOT</b> <i>filesystem:/file-url</i>	—A semicolon-separated list of executable files to try to load and execute when automatically booting up. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot up the first bootable file that it can find in the flash file system.
	<b>ENABLE_BREAK</b>	—Decides whether the automatic bootup process can be interrupted by using the Break key on the console. Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic bootup process by pressing the Break key on the console after the flash file system has initialized.
	<b>HELPER</b> <i>filesystem:/file-url</i>	—A semicolon-separated list of loadable files to dynamically load during the bootloader initialization. Helper files extend or patch the functionality of the bootloader.
	<b>PS1</b> <i>prompt</i>	—A string that is used as the command-line prompt in bootloader mode.
	<b>CONFIG_FILE</b> <i>flash:/file-url</i>	—The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	<b>BAUD</b> <i>rate</i>	—The rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the bootloader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 bps. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000. The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.
	<b>HELPER_CONFIG_FILE</b> <i>filesystem:/file-url</i>	—The name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

**Defaults**

The environment variables have these default values:

MANUAL\_BOOT: No (0)

BOOT: Null string

ENABLE\_BREAK: No (Off or 0) (the automatic bootup process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG\_FILE: config.text

BAUD: 9600 bps

HELPER\_CONFIG\_FILE: No default value (no helper configuration file is specified).

SWITCH\_NUMBER: 1

SWITCH\_PRIORITY: 1

**Note**

Environment variables that have values are stored in the flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, " ") is a variable with a value. Many environment variables are predefined and have default values.

**Command Modes**

Bootloader

**Command History****Usage Guidelines**

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

Under normal circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL\_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system filesystem:/file-url** global configuration command.

The ENABLE\_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper filesystem:/file-url** global configuration command.

The CONFIG\_FILE environment variable can also be set by using the **boot config-file flash:/file-url** global configuration command.

The HELPER\_CONFIG\_FILE environment variable can also be set by using the **boot helper-config-file filesystem:/file-url** global configuration command.

The HELPER\_CONFIG\_FILE environment variable can also be set by using the **boot helper-config-file filesystem:/file-url** global configuration command.

The bootloader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

**set****Examples**

This example shows how to change the bootloader prompt:

```
switch: set PS1 loader:
loader:
```

You can verify your setting by using the **set** bootloader command.

**Related Commands**

Command	Description
<a href="#"><b>unset</b></a>	Resets one or more environment variables to its previous setting.

## type

Use the **type** bootloader command to display the contents of one or more files.

**type** *filesystem:/file-url ...*

<b>Syntax Description</b>	<b>filesystem:</b> Alias for a flash file system. Use <b>flash:</b> for the system board flash device. <b>/file-url</b> Path (directory) and name of the files to display. Separate each filename with a space.
---------------------------	--

<b>Command Modes</b>	Bootloader
----------------------	------------

### Command History

### Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

<b>Examples</b>	This example shows how to display the contents of two files:
-----------------	--

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: image-version
version_directory: image-name
image_name: image-name .bin
ios_image_file_size: 6398464
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128|LAYER_2|MIN_DRAM_MEG=64 switch-family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

### Related Commands

Command	Description
<b>cat</b>	Displays the contents of one or more files.
<b>more</b>	Displays the contents of one or more files.

**unset**

# unset

Use the **unset** bootloader command to reset one or more environment variables.

**unset** *variable* ...

Syntax Description	<i>variable</i>	Use one of these keywords for <i>variable</i> :
	<b>MANUAL_BOOT</b>	Decides whether the switch automatically or manually boots up.
	<b>BOOT</b>	Resets the list of executable files to try to load and execute when automatically booting up. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot up the first bootable file that it can find in the flash file system.
	<b>ENABLE_BREAK</b>	Decides whether the automatic bootup process can be interrupted by using the Break key on the console after the flash file system has been initialized.
	<b>HELPER</b>	A semicolon-separated list of loadable files to dynamically load during the bootloader initialization. Helper files extend or patch the functionality of the bootloader.
	<b>PS1</b>	A string that is used as the command-line prompt in bootloader mode.
	<b>CONFIG_FILE</b>	Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	<b>BAUD</b>	Resets the rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the bootloader and continues to use this value unless the configuration file specifies another setting.
	<b>HELPER_CONFIG_FILE</b>	Resets the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

**Command Modes** Bootloader

**Command History**

**Usage Guidelines**

Under normal circumstances, it is not necessary to alter the setting of the environment variables. The MANUAL\_BOOT environment variable can also be reset by using the **no boot manual** global configuration command. The BOOT environment variable can also be reset by using the **no boot system** global configuration command. The ENABLE\_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command. The HELPER environment variable can also be reset by using the **no boot helper** global configuration command. The CONFIG\_FILE environment variable can also be reset by using the **no boot config-file** global configuration command. The HELPER\_CONFIG\_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command. The bootloader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

**Examples**

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

**Related Commands**

Command	Description
<b>set</b>	Sets or displays environment variables.

**version**

## version

Use the **version** boot loader command to display the bootloader version.

**version**

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

**Command Modes** Bootloader

### Command History

#### Examples

This example shows how to display the bootloader version:

```
switch: version
Compiled Wed 05-Mar-08 10:11 by engineer
```



## Catalyst Switch Debug Commands

This appendix describes the **debug** privileged EXEC commands that have been created or changed for use with the Catalyst switch. These commands are helpful in diagnosing and resolving internetworking problems and should be enabled only under the guidance of Cisco technical support staff.

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

**debug authentication**

# debug authentication

Use the **debug authentication** privileged EXEC command to enable debugging of the authentication settings on an interface. Use the **no** form of this command to disable debugging.

```
debug authentication {all | errors | events | sync | feature [all] [acct] [auth_fail_vlan]
[auth_policy] [autocfg] [critical] [dhcp] [guest_vlan] [mab_pm] [mda] [multi_auth]
[switch_pm] [switch_sync] [vlan_assign] [voice] [webauth] [all | errors | events]}
```

```
no debug authentication {all | errors | events | sync | feature [all] [acct] [auth_fail_vlan]
[auth_policy] [autocfg] [critical] [dhcp] [guest_vlan] [mab_pm] [mda] [multi_auth]
[switch_pm] [switch_sync] [vlan_assign] [voice] [webauth] [all | errors | events]}
```

Syntax Description	acct all auth_fail_vlan auth_policy autocfg critical dhcp errors events feature guest_vlan mab_pm mda multi_auth switch_pm switch_sync sync vlan_assign voice webauth	(Optional) Display authentication manager accounting information. (Optional) Display all authentication manager debug messages. (Optional) Display authentication manager errors for the restricted VLAN. (Optional) Display authentication policy messages. (Optional) Display autoconfiguration authentication manager debug messages. (Optional) Display the inaccessible authentication bypass messages.  <b>Note</b> The inaccessible authentication bypass feature is also referred to as critical authentication or the authentication, authorization, and accounting (AAA) fail policy. (Optional) Display authentication manager debug messages on DHCP dynamic address-enable interfaces. (Optional) Display all authentication manager error debug messages. (Optional) Display all authentication manager event debug messages, including registry and miscellaneous events. (Optional) Display authentication manager feature debug messages (Optional) Display guest VLAN authentication manager messages. (Optional) Display MAC authentication manager bypass authentication debug messages. (Optional) Display multidomain authentication manager debug messages. (Optional) Display multi-authentication manager debug authentication messages. (Optional) Display switch port manager messages. (Optional) Display synchronization messages between the switch, the authentication server, and the connected devices. (Optional) Display operational synchronization authentication manager debug messages. (Optional) Display the VLAN-assignment debug messages. (Optional) Display the voice-VLAN debug messages. (Optional) Display web authentication manager debug messages.
--------------------	--	--

<b>Defaults</b>	Authentication debugging is disabled.																								
<b>Command Modes</b>	Privileged EXEC																								
<b>Command History</b>	<table border="1"> <thead> <tr> <th><b>Release</b></th><th><b>Modification</b></th></tr> </thead> <tbody> <tr> <td>12.2(50)SE</td><td>This command was introduced.</td></tr> </tbody> </table>	<b>Release</b>	<b>Modification</b>	12.2(50)SE	This command was introduced.																				
<b>Release</b>	<b>Modification</b>																								
12.2(50)SE	This command was introduced.																								
<b>Usage Guidelines</b>	The <b>undebug authentication</b> command is the same as the <b>no debug authentication</b> command.																								
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><b>authentication control-direction</b></td><td>Configures the port mode as unidirectional or bidirectional.</td></tr> <tr> <td><b>authentication event</b></td><td>Sets the action for specific authentication events.</td></tr> <tr> <td><b>authentication event linksec fail action</b></td><td>Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.</td></tr> <tr> <td><b>authentication host-mode</b></td><td>Sets the authorization manager mode on a port.</td></tr> <tr> <td><b>authentication open</b></td><td>Enables or disables open access on a port.</td></tr> <tr> <td><b>authentication order</b></td><td>Sets the order of authentication methods used on a port.</td></tr> <tr> <td><b>authentication periodic</b></td><td>Enables or disables reauthentication on a port.</td></tr> <tr> <td><b>authentication port-control</b></td><td>Enables manual control of the port authorization state.</td></tr> <tr> <td><b>authentication priority</b></td><td>Adds an authentication method to the port-priority list.</td></tr> <tr> <td><b>authentication violation</b></td><td>Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.</td></tr> <tr> <td><b>show authentication</b></td><td>Displays information about authentication manager events on the switch.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.	<b>authentication event</b>	Sets the action for specific authentication events.	<b>authentication event linksec fail action</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.	<b>authentication host-mode</b>	Sets the authorization manager mode on a port.	<b>authentication open</b>	Enables or disables open access on a port.	<b>authentication order</b>	Sets the order of authentication methods used on a port.	<b>authentication periodic</b>	Enables or disables reauthentication on a port.	<b>authentication port-control</b>	Enables manual control of the port authorization state.	<b>authentication priority</b>	Adds an authentication method to the port-priority list.	<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.	<b>show authentication</b>	Displays information about authentication manager events on the switch.
<b>Command</b>	<b>Description</b>																								
<b>authentication control-direction</b>	Configures the port mode as unidirectional or bidirectional.																								
<b>authentication event</b>	Sets the action for specific authentication events.																								
<b>authentication event linksec fail action</b>	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.																								
<b>authentication host-mode</b>	Sets the authorization manager mode on a port.																								
<b>authentication open</b>	Enables or disables open access on a port.																								
<b>authentication order</b>	Sets the order of authentication methods used on a port.																								
<b>authentication periodic</b>	Enables or disables reauthentication on a port.																								
<b>authentication port-control</b>	Enables manual control of the port authorization state.																								
<b>authentication priority</b>	Adds an authentication method to the port-priority list.																								
<b>authentication violation</b>	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.																								
<b>show authentication</b>	Displays information about authentication manager events on the switch.																								

**debug auto qos**

# debug auto qos

Use the **debug auto qos** privileged EXEC command to enable debugging of the automatic quality of service (auto-QoS) feature. Use the **no** form of this command to disable debugging.

**debug auto qos**

**no debug auto qos**

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

**Defaults** Auto-QoS debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging *before* you enable auto-QoS. You enable debugging by entering the **debug auto qos** privileged EXEC command.

The **undebug auto qos** command is the same as the **no debug auto qos** command.

## Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```

Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip cisco-phone

21:29:41: mls qos map cos-dscp 0 8 16 26 32 46 48 56
21:29:41: mls qos
21:29:42: no mls qos srr-queue input cos-map
21:29:42: no mls qos srr-queue output cos-map
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 3 0
21:29:42: mls qos srr-queue input cos-map queue 1 threshold 2 1
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 1 2
21:29:42: mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
21:29:43: mls qos srr-queue input cos-map queue 2 threshold 3 3 5
21:29:43: mls qos srr-queue output cos-map queue 1 threshold 3 5
21:29:43: mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
21:29:44: mls qos srr-queue output cos-map queue 3 threshold 3 2 4
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 2 1
21:29:44: mls qos srr-queue output cos-map queue 4 threshold 3 0
21:29:44: no mls qos srr-queue input dscp-map
21:29:44: no mls qos srr-queue output dscp-map
21:29:44: mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7

```

```

21:29:45: mls qos srr-queue input dscp-map queue 1 threshold 3 32
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
21:29:45: mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
21:29:46: mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
21:29:47: mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
21:29:48: mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
21:29:48: mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 1 8
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
21:29:49: mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
21:29:49: no mls qos srr-queue input priority-queue 1
21:29:49: no mls qos srr-queue input priority-queue 2
21:29:50: mls qos srr-queue input bandwidth 90 10
21:29:50: no mls qos srr-queue input buffers
21:29:50: mls qos queue-set output 1 buffers 10 10 26 54
21:29:50: interface GigabitEthernet0/1
21:29:50: mls qos trust device cisco-phone
21:29:50: mls qos trust cos
21:29:50: no queue-set 1
21:29:50: srr-queue bandwidth shape 10 0 0 0
21:29:50: srr-queue bandwidth share 10 10 60 20

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>auto qos voip</b>	Configures auto-QoS for voice over IP (VoIP) within a QoS domain.
<b>show auto qos</b>	Displays the initial configuration that is generated by the automatic auto-QoS feature
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

**debug backup**

# debug backup

Use the **debug backup** privileged EXEC command to enable debugging of the Flex Links backup interface. Use the **no** form of this command to disable debugging.

**debug backup {all | errors | events | vlan-load-balancing}**

**no debug backup {all | errors | events | vlan-load-balancing}**

Syntax Description	<b>all</b> Display all backup interface debug messages.
<b>errors</b>	Display backup interface error or exception debug messages.
<b>events</b>	Display backup interface event debug messages.
<b>vlan-load-balancing</b>	Display backup interface VLAN load balancing.

**Defaults** Backup interface debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

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

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

# debug cisp

Use the **debug cisp** global configuration command to enable debugging message exchanges and events on a Client Information Signalling Protocol (CISP)-enabled interface. Use the **no** form of this command to disable debugging.

**debug cisp [all | errors | events | packets | sync]**

**no debug cisp [initialization | interface-configuration | rpc]**

Syntax Description	<b>all</b> Display all CISP debug messages. <b>errors</b> Display CISP debug messages. <b>events</b> Display CISP event debug messages. <b>packets</b> Display CISP packet debug messages. <b>sync</b> Display CISP operational synchronization debug messages.
--------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	The <b>undebug cisp</b> command is the same as the <b>no debug cisp</b> command.
-------------------------	--

Related Commands	Command	Description
	<b>cisp enable</b>	Enables Client Information Signalling Protocol (CISP)
	<b>dot1x credentials (global configuration) profile</b>	Configures a profile on a supplicant switch.
	<b>show cisp</b>	Displays CISP information for a specified interface.

**debug cluster**

# debug cluster

Use the **debug cluster** privileged EXEC command to enable debugging of cluster-specific events. Use the **no** form of this command to disable debugging.

```
debug cluster {discovery | events | extended | hsrp | http | ip [packet] | members | nat | neighbors | platform | snmp | vqpxy}
```

```
no debug cluster {discovery | events | extended | hsrp | http | ip [packet] | members | nat | neighbors | platform | snmp | vqpxy}
```

Syntax Description	
<b>discovery</b>	Display cluster discovery debug messages.
<b>events</b>	Display cluster event debug messages.
<b>extended</b>	Display extended discovery debug messages.
<b>hsrp</b>	Display the Hot Standby Router Protocol (HSRP) debug messages.
<b>http</b>	Display Hypertext Transfer Protocol (HTTP) debug messages.
<b>ip [packet]</b>	Display IP or transport packet debug messages.
<b>members</b>	Display cluster member debug messages.
<b>nat</b>	Display Network Address Translation (NAT) debug messages.
<b>neighbors</b>	Display cluster neighbor debug messages.
<b>platform</b>	Display platform-specific cluster debug messages.
<b>snmp</b>	Display Simple Network Management Protocol (SNMP) debug messages.
<b>vqpxy</b>	Display VLAN Query Protocol (VQP) proxy debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

This command is available only on the cluster command switch.

The **undebug cluster** command is the same as the **no debug cluster** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show cluster</b>	Displays the cluster status and a summary of the cluster to which the switch belongs.
<b>show cluster candidates</b>	Displays a list of candidate switches when entered on the command switch.
<b>show cluster members</b>	Displays information about cluster members when executed on the command switch.



**debug dot1x**

## debug dot1x

Use the **debug dot1x** privileged EXEC command to enable debugging of the IEEE 802.1x authentication feature. Use the **no** form of this command to disable debugging.

**debug dot1x {all | errors | events | feature | packets | registry | state-machine}**

**no debug dot1x {all | errors | events | feature | packets | registry | state-machine}**

Syntax Description	<b>all</b> Display all IEEE 802.1x authentication debug messages.
<b>errors</b>	Display IEEE 802.1x error debug messages.
<b>events</b>	Display IEEE 802.1x event debug messages.
<b>feature</b>	Display IEEE 802.1x feature debug messages.
<b>packets</b>	Display IEEE 802.1x packet debug messages.
<b>registry</b>	Display IEEE 802.1x registry invocation debug messages.
<b>state-machine</b>	Display state-machine related-events debug messages.



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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(25)SEE	The <b>feature</b> keyword was added.

**Usage Guidelines** The **undebug dot1x** command is the same as the **no debug dot1x** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show dot1x</b>	Displays IEEE 802.1xstatistics, administrative status, and operational status for the switch or for the specified port.

**debug dtp**

# debug dtp

Use the **debug dtp** privileged EXEC command to enable debugging of the Dynamic Trunking Protocol (DTP) activity. Use the **no** form of this command to disable debugging.

**debug dtp {aggregation | all | decision | events | oserrs | packets | queue | states | timers}**

**no debug dtp {aggregation | all | decision | events | oserrs | packets | queue | states | timers}**

<b>Syntax Description</b>	
<b>aggregation</b>	Display DTP user-message aggregation debug messages.
<b>all</b>	Display all DTP debug messages.
<b>decision</b>	Display the DTP decision-table debug messages.
<b>events</b>	Display the DTP event debug messages.
<b>oserrs</b>	Display DTP operating system-related error debug messages.
<b>packets</b>	Display DTP packet-processing debug messages.
<b>queue</b>	Display DTP packet-queueing debug messages.
<b>states</b>	Display DTP state-transition debug messages.
<b>timers</b>	Display DTP timer-event debug messages.

<b>Defaults</b>	Debugging is disabled.
<b>Command Modes</b>	Privileged EXEC

<b>Command History</b>	
<b>Usage Guidelines</b>	The <b>undebug dtp</b> command is the same as the <b>no debug dtp</b> command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show dtp</b>	Displays DTP information for the switch or for a specified interface.

# debug eap

Use the **debug eap** privileged EXEC command to enable debugging of the Extensible Authentication Protocol (EAP) activity. Use the **no** form of this command to disable debugging.

**debug dot1x {all | authenticator | errors | events | md5 | packets | peer | sm}**

**no debug dot1x {all | authenticator | errors | events | md5 | packets | peer | sm}**

Syntax Description	<b>all</b> Display all EAP debug messages. <b>authenticator</b> Display authenticator debug messages. <b>errors</b> Display EAP error debug messages. <b>events</b> Display EAP event debug messages. <b>md5</b> Display EAP-MD5 debug messages. <b>packets</b> Display EAP packet debug messages. <b>peer</b> Display EAP peer debug messages. <b>sm</b> Display EAP state-machine related-events debug messages.
--------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(25)SEE	This command was introduced.

<b>Usage Guidelines</b>	The <b>undebug dot1x</b> command is the same as the <b>no debug dot1x</b> command.
-------------------------	--

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show eap</b>	Displays EAP registration and session information for the switch or for the specified port.

**debug etherchannel**

# debug etherchannel

Use the **debug etherchannel** privileged EXEC command to enable debugging of the EtherChannel/PAgP shim. This shim is the software module that is the interface between the Port Aggregation Protocol (PAgP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

**debug etherchannel [all | detail | error | event | idb]**

**no debug etherchannel [all | detail | error | event | idb]**

---

**Syntax Description**

<b>all</b>	(Optional) Display all EtherChannel debug messages.
<b>detail</b>	(Optional) Display detailed EtherChannel debug messages.
<b>error</b>	(Optional) Display EtherChannel error debug messages.
<b>event</b>	(Optional) Debug major EtherChannel event messages.
<b>idb</b>	(Optional) Display PAgP interface descriptor block debug messages.

---



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

---



---

**Defaults**

Debugging is disabled.

---

**Command Modes**

Privileged EXEC

---

**Command History**
**Usage Guidelines**

If you do not specify a keyword, all debug messages appear.

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

---

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show etherchannel</b>	Displays EtherChannel information for the channel.

---

# debug ilpower

Use the **debug ilpower** privileged EXEC command to enable debugging of the power controller and Power over Ethernet (PoE) system. Use the **no** form of this command to disable debugging.

**debug ilpower {cdp | controller | event | ha | port | powerman | registries}**

**no debug ilpower {cdp | controller | event | ha | port | powerman | registries}**

Syntax Description	<b>cdp</b> Display PoE Cisco Discovery Protocol (CDP) debug messages. <b>controller</b> Display PoE controller debug messages. <b>event</b> Display PoE event debug messages. <b>ha</b> Display PoE high-availability messages. <b>port</b> Display PoE port manager debug messages. <b>powerman</b> Display PoE power management debug messages. <b>registries</b> Display PoE registries debug messages.
--------------------	--

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

**Usage Guidelines**      This command is supported only on PoE-capable switches.

Related Commands	Command	Description
	<b>show controllers power inline</b>	Displays the values in the registers of the specified PoE controller.
	<b>show power inline</b>	Displays the power status for the specified PoE port or for all PoE ports.

**debug interface**

# debug interface

Use the **debug interface** privileged EXEC command to enable debugging of interface-related activities. Use the **no** form of this command to disable debugging.

```
debug interface {interface-id | null interface-number | port-channel port-channel-number |
vlan vlan-id}
```

```
no debug interface {interface-id | null interface-number | port-channel port-channel-number |
vlan vlan-id}
```

<b>Syntax Description</b>	<p><b>interface-id</b> Display debug messages for the specified physical port, identified by type switch number/module number/ port, for example <b>gigabitethernet 0/2</b>.</p> <p><b>null interface-number</b> Display debug messages for null interfaces. The <i>interface-number</i> is always <b>0</b>.</p> <p><b>port-channel port-channel-number</b> Display debug messages for the specified EtherChannel port-channel interface. The <i>port-channel-number</i> range is 1 to .</p> <p><b>vlan vlan-id</b> Display debug messages for the specified VLAN. The <i>vlan-id</i> range is 1 to 4094.</p>
---------------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

**Command History**

If you do not specify a keyword, all debug messages appear.

The **undebbug interface** command is the same as the **no debug interface** command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show etherchannel</b>	Displays EtherChannel information for the channel.

# debug ip dhcp snooping

Use the **debug ip dhcp snooping** privileged EXEC command to enable debugging of DHCP snooping. Use the **no** form of this command to disable debugging.

**debug ip dhcp snooping {mac-address | agent | event | packet}**

**no debug ip dhcp snooping {mac-address | agent | event | packet}**

<b>Syntax Description</b>	<i>mac-address</i> Display debug messages for a DHCP packet with the specified MAC address. <i>agent</i> Display debug messages for DHCP snooping agents. <i>event</i> Display debug messages for DHCP snooping events. <i>packet</i> Display debug messages for DHCP snooping.
---------------------------	--

**Defaults**              Debugging is disabled.

**Command Modes**        Privileged EXEC

## Command History

**Usage Guidelines**      The **undebug ip dhcp snooping** command is the same as the **no debug ip dhcp snooping** command.

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

■ **debug ip verify source packet**

# debug ip verify source packet

Use the **debug ip verify source packet** privileged EXEC command to enable debugging of IP source guard. Use the **no** form of this command to disable debugging.

**debug ip verify source packet**

**no debug ip verify source packet**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **undebug ip verify source packet** command is the same as the **no debug ip verify source packet** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug ip igmp filter

Use the **debug ip igmp filter** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) filter events. Use the **no** form of this command to disable debugging.

**debug ip igmp filter**

**no debug ip igmp filter**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **undebug ip igmp filter** command is the same as the **no debug ip igmp filter** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

■ **debug ip igmp max-groups**

## debug ip igmp max-groups

Use the **debug ip igmp max-groups** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) maximum groups events. Use the **no** form of this command to disable debugging.

**debug ip igmp max-groups**

**no debug ip igmp max-groups**

---

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

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

**Command History**

**Usage Guidelines** The **undebug ip igmp max-groups** command is the same as the **no debug ip igmp max-groups** command.

---

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

# debug ip igmp snooping

Use the **debug igmp snooping** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) snooping activity. Use the **no** form of this command to disable debugging.

**debug ip igmp snooping [group | management | querier | router | timer]**

**no debug ip igmp snooping [group | management | querier | router | timer]**

<b>Syntax Description</b>	<b>group</b> (Optional) Display IGMP snooping group activity debug messages. <b>management</b> (Optional) Display IGMP snooping management activity debug messages. <b>querier</b> (Optional) Display IGMP snooping querier debug messages. <b>router</b> (Optional) Display IGMP snooping router activity debug messages. <b>timer</b> (Optional) Display IGMP snooping timer event debug messages.
---------------------------	--

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **undebbug ip igmp snooping** command is the same as the **no debug ip igmp snooping** command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>debug platform ip igmp snooping</b>	Displays information about platform-dependent IGMP snooping activity.
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

**debug lacp**

## debug lacp

Use the **debug lacp** privileged EXEC command to enable debugging of Link Aggregation Control Protocol (LACP) activity. Use the **no** form of this command to disable debugging.

**debug lacp [all | event | fsm | misc | packet]**

**no debug lacp [all | event | fsm | misc | packet]**

Syntax Description	<b>all</b> (Optional) Display all LACP debug messages.
<b>event</b>	(Optional) Display LACP event debug messages.
<b>fsm</b>	(Optional) Display LACP finite state-machine debug messages.
<b>misc</b>	(Optional) Display miscellaneous LACP debug messages.
<b>packet</b>	(Optional) Display LACP packet debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

### Command History

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

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show lacp</b>	Displays LACP channel-group information.

# debug lldp packets

Use the **debug lldp packets** privileged EXEC command to enable debugging of Link Layer Discovery Protocol (LLDP) packets. Use the **no** form of this command to disable debugging.

**debug lldp packets**

**no debug lldp packets**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

**Usage Guidelines** The **undebbug lldp packets** command is the same as the **no debug lldp packets** command.

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

**debug mac-notification**

# debug mac-notification

Use the **debug mac-notification** privileged EXEC command to enable debugging of MAC notification events. Use the **no** form of this command to disable debugging.

**debug mac-notification**

**no debug mac-notification**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines** The **undebug mac-notification** command is the same as the **no debug mac-notification** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show mac address-table notification</b>	Displays the MAC address notification information for all interfaces or the specified interface.

# debug matm

Use the **debug matm** privileged EXEC command to enable debugging of platform-independent MAC address management. Use the **no** form of this command to disable debugging.

**debug matm**

**no debug matm**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

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

## Related Commands

Command	Description
<a href="#">debug platform matm</a>	Displays information about platform-dependent MAC address management.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

■ **debug matm move update**

# debug matm move update

Use the **debug matm move update** privileged EXEC command to enable debugging of MAC address-table move update message processing.

**debug matm move update**

**no debug matm move update**

---

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

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(25)SED	This command was introduced.

---

**Usage Guidelines** The **undebug matm move update** command is the same as the **no debug matm move update** command.

---

Related Commands	Command	Description
	<b>mac address-table move update {receive   transmit}</b>	Configures MAC address-table move update feature on the switch.
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show mac address-table move update</b>	Displays the MAC address-table move update information on the switch.

# debug monitor

Use the **debug monitor** privileged EXEC command to enable debugging of the Switched Port Analyzer (SPAN) feature. Use the **no** form of this command to disable debugging.

**debug monitor {all | errors | idb-update | info | list | notifications | platform | requests | snmp}**

**no debug monitor {all | errors | idb-update | info | list | notifications | platform | requests | snmp}**

Syntax Description	<b>all</b> Display all SPAN debug messages.
<b>errors</b>	Display detailed SPAN error debug messages.
<b>idb-update</b>	Display SPAN interface description block (IDB) update-trace debug messages.
<b>info</b>	Display SPAN informational-tracing debug messages.
<b>list</b>	Display SPAN port and VLAN-list tracing debug messages.
<b>notifications</b>	Display SPAN notification debug messages.
<b>platform</b>	Display SPAN platform-tracing debug messages.
<b>requests</b>	Display SPAN request debug messages.
<b>snmp</b>	Display SPAN and Simple Network Management Protocol (SNMP) tracing debug messages.

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	The <b>undebug monitor</b> command is the same as the <b>no debug monitor</b> command.
-------------------------	--

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show monitor</b>	Displays information about all SPAN and remote SPAN (RSPAN) sessions on the switch.

**debug mvrdbg**

## debug mvrdbg

Use the **debug mvrdbg** privileged EXEC command to enable debugging of Multicast VLAN Registration (MVR). Use the **no** form of this command to disable debugging.

**debug mvrdbg {all | events | igmpsn | management | ports}**

**no debug mvrdbg {all | events | igmpsn | management | ports}**

Syntax Description	<b>all</b> Display all MVR activity debug messages.
<b>events</b>	Display MVR event-handling debug messages.
<b>igmpsn</b>	Display MVR Internet Group Management Protocol (IGMP) snooping-activity debug messages.
<b>management</b>	Display MVR management-activity debug messages.
<b>ports</b>	Display MVR port debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

### Command History

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

### Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show mvr</b>	Displays the current MVR configuration.

# debug nmsp

Use the **debug nmsp** privileged EXEC command to enable debugging of the Network Mobility Services Protocol (NMSP) on the switch. This command is available only when your switch is running the cryptographic (encrypted) software image. Use the **no** form of this command to disable debugging.

**debug nmsp {all | connection | error | event | packet | rx | tx}**

**no debug nmsp**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(50)SE	This command was introduced.

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

Related Commands	Command	Description
	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.
	<a href="#">show nmsp</a>	Displays the NMSP information.

**debug nvram**

## debug nvram

Use the **debug nvram** privileged EXEC command to enable debugging of NVRAM activity. Use the **no** form of this command to disable debugging.

**debug nvram**

**no debug nvram**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

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

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug pagp

Use the **debug pagp** privileged EXEC command to enable debugging of Port Aggregation Protocol (PAgP) activity. Use the **no** form of this command to disable debugging.

**debug pagp [all | dual-active | event | fsm | misc | packet]**

**no debug pagp [all | dual-active | event | fsm | misc | packet]**

Syntax Description	<b>all</b> (Optional) Display all PAgP debug messages. <b>dual-active</b> (Optional) Display dual-active detection messages. <b>event</b> (Optional) Display PAgP event debug messages. <b>fsm</b> (Optional) Display PAgP finite state-machine debug messages. <b>misc</b> (Optional) Display miscellaneous PAgP debug messages. <b>packet</b> (Optional) Display PAgP packet debug messages.
--------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(46)SE	The <b>dual-active</b> keyword was added.

<b>Usage Guidelines</b>	The <b>undebug pagp</b> command is the same as the <b>no debug pagp</b> command.
-------------------------	--

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show pagp</b>	Displays PAgP channel-group information.

**debug platform acl**

# debug platform acl

Use the **debug platform acl** privileged EXEC command to enable debugging of the access control list (ACL) manager. Use the **no** form of this command to disable debugging.

```
debug platform acl {all | exit | label | main | warn}
no debug platform acl {all | exit | label | main | warn}
```

Syntax Description	<b>all</b> Display all ACL manager debug messages. <b>exit</b> Display ACL exit-related debug messages. <b>label</b> Display ACL label-related debug messages. <b>main</b> Display the main or important ACL debug messages. <b>warn</b> Display ACL warning-related debug messages.
--------------------	--

---

**Defaults**                  Debugging is disabled.

---

**Command Modes**              Privileged EXEC

---

**Command History**

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

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

# debug platform backup interface

Use the **debug platform backup interface** privileged EXEC command to enable debugging of the Flex Links platform backup interface. Use the **no** form of this command to disable debugging.

**debug platform backup interface**

**no debug platform backup interface**

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

**Defaults** Platform backup interface debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

■ **debug platform cisp**

# debug platform cisp

Use the **debug platform cisp** global configuration command to enable platform-level debugging of a switch that has one or more Client Information Signalling Protocol (CISP)-enabled interfaces. Use the **no** form of this command to disable debugging.

**debug platform cisp [initialization | interface-configuration | rpc]**

**no debug platform cisp [initialization | interface-configuration | rpc]**

<b>Syntax Description</b>	<b>initialization</b> Enable debugging of the CISP initialization sequence. <b>interface-configuration</b> Enable debugging of the CISP configuration. <b>rpc</b> Enable debugging of the CISP RPC requests.
---------------------------	--

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

**Usage Guidelines**      The **undebbug platform cisp** command is the same as the **no debug platform cisp** command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#"><b>cisp enable</b></a>	Enables Client Information Signalling Protocol (CISP)
	<a href="#"><b>dot1x credentials (global configuration)profile</b></a>	Configures a profile on a supplicant switch.
	<a href="#"><b>show cisp</b></a>	Displays CISP information for a specified interface.

# debug platform cpu-queues

Use the **debug platform cpu-queues** privileged EXEC command to enable debugging of platform central processing unit (CPU) receive queues. Use the **no** form of this command to disable debugging.

```
debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
    igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | software-fwd-q |
    stp-q}
```

```
no debug platform cpu-queues {broadcast-q | cbt-to-spt-q | cpuhub-q | host-q | icmp-q |
    igmp-snooping-q | layer2-protocol-q | logging-q | remote-console-q | software-fwd-q |
    stp-q}
```

Syntax Description	
<b>broadcast-q</b>	Display debug messages about packets received by the broadcast queue.
<b>cbt-to-spt-q</b>	Display debug messages about packets received by the core-based tree to shortest-path tree (cbt-to-spt) queue.
<b>cpuhub-q</b>	Display debug messages about packets received by the CPU heartbeat queue.
<b>host-q</b>	Display debug messages about packets received by the host queue.
<b>icmp-q</b>	Display debug messages about packets received by the Internet Control Message Protocol (ICMP) queue.
<b>igmp-snooping-q</b>	Display debug messages about packets received by the Internet Group Management Protocol (IGMP)-snooping queue.
<b>layer2-protocol-q</b>	Display debug messages about packets received by the Layer 2 protocol queue.
<b>logging-q</b>	Display debug messages about packets received by the logging queue.
<b>remote-console-q</b>	Display debug messages about packets received by the remote console queue.
<b>software-fwd-q</b>	Debug packets received by the software forwarding queue.
<b>stp-q</b>	Debug packets received by the Spanning Tree Protocol (STP) queue.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **undebug platform cpu-queues** command is the same as the **no debug platform cpu-queues** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

■ **debug platform dot1x**

## debug platform dot1x

Use the **debug platform dot1x** privileged EXEC command to enable debugging of IEEE 802.1x events. Use the **no** form of this command to disable debugging.

**debug platform dot1x {initialization | interface-configuration | rpc}**

**no debug platform dot1x {initialization | interface-configuration | rpc}**

<b>Syntax Description</b>	<b>initialization</b> Display IEEE 802.1x-authentication initialization sequence debug messages. <b>interface-configuration</b> Display IEEE 802.1x interface configuration-related debug messages. <b>rpc</b> Display IEEE 802.1x remote procedure call (RPC) request debug messages.
---------------------------	--

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

### Command History

The **undebug platform dot1x** command is the same as the **no debug platform dot1x** command.

### Related Commands

<b>Command</b>	<b>Description</b>
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform etherchannel

Use the **debug platform etherchannel** privileged EXEC command to enable debugging of platform-dependent EtherChannel events. Use the **no** form of this command to disable debugging.

**debug platform etherchannel {init | link-up | rpc | warnings}**

**no debug platform etherchannel {init | link-up | rpc | warnings}**

<b>Syntax Description</b>	<b>init</b> Display EtherChannel module initialization debug messages. <b>link-up</b> Display EtherChannel link-up and link-down related debug messages. <b>rpc</b> Display EtherChannel remote procedure call (RPC) debug messages. <b>warnings</b> Display EtherChannel warning debug messages.
---------------------------	--

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

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

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

---

 debug platform forw-tcam

# debug platform forw-tcam

Use the **debug platform forw-tcam** privileged EXEC command to enable debugging of the forwarding ternary content addressable memory (TCAM) manager. Use the **no** form of this command to disable debugging.

**debug platform forw-tcam [adjustment | allocate | audit | error | move | read | write]**

**no debug platform forw-tcam [adjustment | allocate | audit | error | move | read | write]**

Syntax Description	adjustment      (Optional) Display TCAM manager adjustment debug messages.
allocate	(Optional) Display TCAM manager allocation debug messages.
audit	(Optional) Display TCAM manager audit messages.
error	(Optional) Display TCAM manager error messages.
move	(Optional) Display TCAM manager move messages.
read	(Optional) Display TCAM manager read messages.
write	(Optional) Display TCAM manager write messages.

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

**Command History**

**Usage Guidelines** If you do not specify a keyword, all forwarding TCAM manager debug messages appear.

The **undebug platform forw-tcam** command is the same as the **no debug platform forw-tcam** command.

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

# debug platform frontend-controller

Use the **debug platform frontend-controller** privileged EXEC command to enable debugging of front-end controller activity. Use the **no** form of this command to disable debugging.

**debug platform frontend-controller {all | image | led | manager | poe | register | thermal}**

**no debug platform frontend-controller {all | image | led | manager | poe | register | thermal}**

Syntax Description	<b>all</b> Display all the debug messages for front-end controller. <b>image</b> Display Image Manager debug messages. <b>led</b> Display LED debug messages. <b>manager</b> Display front-end-controller manager debug messages. <b>poe</b> Display Power over Ethernet (PoE) debug messages. <b>register</b> Display Register Access debug messages. <b>thermal</b> Display thermal debug messages.
--------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	This command is only supported on Power over Ethernet switches.
-------------------------	---

The **undebug platform frontend-controller** command is the same as the **no debug platform frontend-controller** command.

Related Commands	Command	Description
	<b>show platform frontend-controller</b>	Displays counter and status information for the front-end controller manager and subordinate applications, and displays the hardware and software information for the front-end controller.
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

■ **debug platform ip arp inspection**

# debug platform ip arp inspection

Use the **debug platform ip arp inspection** privileged EXEC command to debug dynamic Address Resolution Protocol (ARP) inspection events. Use the **no** form of this command to disable debugging.

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

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

Syntax Description	<b>all</b> Display all dynamic ARP inspection debug messages. <b>error</b> Display dynamic ARP inspection error debug messages. <b>event</b> Display dynamic ARP inspection event debug messages. <b>packet</b> Display dynamic ARP inspection packet-related debug messages. <b>rpc</b> Display dynamic ARP inspection remote procedure call (RPC) request debug messages.
--------------------	---

---

**Defaults**      Debugging is disabled.

---

**Command Modes**      Privileged EXEC

---

**Command History**

**Usage Guidelines**      The **udebug platform ip arp inspection** command is the same as the **no debug platform ip arp inspection** command.

Related Commands	Command	Description
	<b>show interfaces transceivers</b>	Displays the dynamic ARP inspection configuration and operating state.
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform ip dhcp

Use the **debug platform ip dhcp** privileged EXEC command to debug DHCP events. Use the **no** form of this command to disable debugging.

**debug platform ip dhcp [all | error | event | packet | rpc]**

**no debug platform ip dhcp [all | error | event | packet | rpc]**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

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

## Related Commands

Command	Description
<a href="#">show ip dhcp snooping</a>	Displays the DHCP snooping configuration.
<a href="#">show ip dhcp snooping binding</a>	Displays the DHCP snooping binding information.
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

---

```
■ debug platform ip igmp snooping
```

# debug platform ip igmp snooping

Use the **debug platform ip igmp snooping** privileged EXEC command to enable debugging of platform-dependent Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable debugging.

```
debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

```
debug platform ip igmp snooping pak {ip-address | error | ipopt | leave | query | report | rx | svi | tx}
```

```
debug platform ip igmp snooping rpc [cfg | misc | vlan]
```

```
no debug platform ip igmp snooping {all | di | error | event | group | mgmt | pak | retry | rpc | warn}
```

Syntax Description	
<b>all</b>	Display all IGMP snooping debug messages.
<b>di</b>	Display IGMP snooping destination index (di) coordination remote procedure call (RPC) debug messages.
<b>error</b>	Display IGMP snooping error messages.
<b>event</b>	Display IGMP snooping event debug messages.
<b>group</b>	Display IGMP snooping group debug messages.
<b>mgmt</b>	Display IGMP snooping management debug messages.
<b>pak {ip-address   error   ipopt   leave   query   report   rx   svi   tx}</b>	Display IGMP snooping packet event debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>ip-address</b>—IP address of the IGMP group.</li> <li>• <b>error</b>—Display IGMP snooping packet error debug messages.</li> <li>• <b>ipopt</b>—Display IGMP snooping IP bridging options debug messages.</li> <li>• <b>leave</b>—Display IGMP snooping leave debug messages.</li> <li>• <b>query</b>—Display IGMP snooping query debug messages.</li> <li>• <b>report</b>—Display IGMP snooping report debug messages.</li> <li>• <b>rx</b>—Display IGMP snooping received packet debug messages.</li> <li>• <b>svi</b>—Display IGMP snooping switched virtual interface (SVI) packet debug messages.</li> <li>• <b>tx</b>—Display IGMP snooping sent packet debug messages.</li> </ul>
<b>retry</b>	Display IGMP snooping retry debug messages.
<b>rpc [cfg   misc   vlan]</b>	Display IGMP snooping remote procedure call (RPC) event debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>cfg</b>—(Optional) Display IGMP snooping RPC debug messages.</li> <li>• <b>misc</b>—(Optional) IGMP snooping miscellaneous RPC debug messages.</li> <li>• <b>vlan</b>—(Optional) IGMP snooping VLAN assert RPC debug messages.</li> </ul>
<b>warn</b>	Display IGMP snooping warning messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines** The **undebug platform ip igmp snooping** command is the same as the **no debug platform ip igmp snooping** command.

**Related Commands**

Command	Description
<b>debug ip igmp snooping</b>	Displays information about platform-independent IGMP snooping activity.
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

 ■ debug platform ip source-guard

# debug platform ip source-guard

Use the **debug platform ip source-guard** privileged EXEC command to debug IP source guard events.  
Use the **no** form of this command to disable debugging.

**debug platform ip source-guard {all | error | event}**

**no debug platform ip source-guard {all | error | event }**

<b>Syntax Description</b>	<b>all</b> Display all IP source-guard platform debug messages. <b>error</b> Display IP source-guard platform error debug messages. <b>event</b> Display IP source-guard platform event debug messages.
---------------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(50)SE	This command was introduced.

<b>Usage Guidelines</b>	The <b>udebug platform ip source-guard</b> command is the same as the <b>no debug platform ip source-guard</b> command.
-------------------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show ip verify source</a>	Displays the IP source guard configuration.
	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.

# debug platform led

Use the **debug platform led** privileged EXEC command to enable debugging of light-emitting diode (LED) actions. Use the **no** form of this command to disable debugging.

**debug platform led {generic | signal}**

**no debug platform led {generic | signal}**

<b>Syntax Description</b>	<b>generic</b> Display LED generic action debug messages. <b>signal</b> Display LED signal bit map debug messages.
---------------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

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

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

■ **debug platform matm**

# debug platform matm

Use the **debug platform matm** privileged EXEC command to enable debugging of platform-dependent MAC address management. Use the **no** form of this command to disable debugging.

**debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address | warnings}**

**no debug platform matm {aging | all | ec-aging | errors | learning | rpc | secure-address | warnings}**

Syntax Description	aging      Display MAC address aging debug messages.
<b>all</b>	Display all platform MAC address management event debug messages.
<b>ec-aging</b>	Display EtherChannel address aging-related debug messages.
<b>errors</b>	Display MAC address management error messages.
<b>learning</b>	Display MAC address management address-learning debug messages.
<b>rpc</b>	Display MAC address management remote procedure call (RPC) related debug messages.
<b>secure-address</b>	Display MAC address management secure address learning debug messages.
<b>warning</b>	Display MAC address management warning messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

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

Related Commands	Command	Description
	<b>debug matm</b>	Displays information about platform-independent MAC address management.
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.

# debug platform messaging application

Use the **debug platform messaging application** privileged EXEC command to enable debugging of application messaging activity. Use the **no** form of this command to disable debugging.

**debug platform messaging application {all | badpak | cleanup | events | memerr | messages | usererr}**

**no debug platform messaging application {all | badpak | cleanup | events | memerr | messages | usererr}**

Syntax Description	<b>all</b> Display all application-messaging debug messages.
<b>badpak</b>	Display bad-packet debug messages.
<b>cleanup</b>	Display clean-up debug messages.
<b>events</b>	Display event debug messages.
<b>memerr</b>	Display memory-error debug messages.
<b>messages</b>	Display application-messaging debug messages.
<b>usererr</b>	Display user-error debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **udebug platform messaging application** command is the same as the **no debug platform messaging application** command.

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

■ **debug platform phy**

# debug platform phy

Use the **debug platform phy** privileged EXEC command to enable debugging of PHY driver information. Use the **no** form of this command to disable debugging.

```
debug platform phy {automdix | cablediag | dual-purpose | flcd {configure | ipc | iter | trace} | flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed | write | xenpak}
```

```
no debug platform phy {automdix | cablediag | dual-purpose | flcd {configure | ipc | iter | trace} | flowcontrol | forced | init-seq | link-status | read | sfp | show-controller | speed | write | xenpak}
```

Syntax Description	<b>automdix</b>	Display PHY automatic medium-dependent interface crossover (auto-MDIX) debug messages.
	<b>cablediag</b>	Display PHY cable-diagnostic debug messages.
	<b>dual-purpose</b>	Display PHY dual-purpose event debug messages.
	<b>flcd {configure   ipc   iter   trace}</b>	Display PHY FLCD debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>configure</b>—Display PHY configure debug messages.</li> <li>• <b>ipc</b>—Display Interprocess Communication Protocol (IPC) debug messages.</li> <li>• <b>iter</b>—Display iter debug messages.</li> <li>• <b>trace</b>—Display trace debug messages.</li> </ul>
	<b>flowcontrol</b>	Display PHY flowcontrol debug messages.
	<b>forced</b>	Display PHY forced-mode debug messages.
	<b>init-seq</b>	Display PHY initialization-sequence debug messages.
	<b>link-status</b>	Display PHY link-status debug messages.
	<b>read</b>	Display PHY-read debug messages.
	<b>sfp</b>	Display PHY small form-factor pluggable (SFP) modules debug messages.
	<b>show-controller</b>	Display PHY show-controller debug messages.
	<b>speed</b>	Display PHY speed-change debug messages.
	<b>write</b>	Display PHY-write debug messages.
	<b>xenpak</b>	Display PHY XENPAK debug messages

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines** The **udebug platform phy** command is the same as the **no debug platform phy** command.

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

■ debug platform pm

# debug platform pm

Use the **debug platform pm** privileged EXEC command to enable debugging of the platform-dependent port manager software module. Use the **no** form of this command to disable debugging.

```
debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events | idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-span | pm-vectors [detail] | rpc [general | oper-info | state | vectors | vp-events] | soutput-vectors | sync | vlans}
```

```
no debug platform pm {all | counters | errdisable | etherchnl | exceptions | hpm-events | idb-events | if-numbers | ios-events | link-status | platform | pm-events | pm-span | pm-vectors [detail] | rpc [general | oper-info | state | vectors | vp-events] | soutput-vectors | sync | vlans}
```

Syntax Description	
<b>all</b>	Display all port-manager debug messages.
<b>counters</b>	Display counters for remote procedure call (RPC) debug messages.
<b>errdisable</b>	Display error-disabled related-events debug messages.
<b>etherchnl</b>	Display EtherChannel related-events debug messages.
<b>exceptions</b>	Display system exception debug messages.
<b>hpm-events</b>	Display platform port-manager event debug messages.
<b>idb-events</b>	Display interface descriptor block (IDB) related-events debug messages.
<b>if-numbers</b>	Display interface-number translation-event debug messages.
<b>ios-events</b>	Display Cisco IOS event debug messages.
<b>link-status</b>	Display interface link-detection event debug messages.
<b>platform</b>	Display port-manager function-event debug messages.
<b>pm-events</b>	Display port manager event debug messages.
<b>pm-span</b>	Display port manager Switched Port Analyzer (SPAN) event debug messages.
<b>pm-vectors [detail]</b>	Display port-manager vector-related-event debug messages. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>detail</b>—Display vector-function details.</li> </ul>
<b>rpc [general   oper-info   state   vectors   vp-events]</b>	Display RPC related-event debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>general</b>—(Optional) Display RPC general events.</li> <li>• <b>oper-info</b>—(Optional) Display operational- and informational-related RPC messages.</li> <li>• <b>state</b>—(Optional) Display administrative- and operational-related RPC messages.</li> <li>• <b>vectors</b>—(Optional) Display vector-related RPC messages.</li> <li>• <b>vp-events</b>—(Optional) Display virtual ports related-events RP messages.</li> </ul>
<b>soutput-vectors</b>	Display IDB output vector event debug messages.
<b>sync</b>	Display operational synchronization and VLAN line-state event debug messages.
<b>vlans</b>	Display VLAN creation and deletion event debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines** The **undebbug platform pm** command is the same as the **no debug platform pm** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

■ **debug platform port-asic**

# debug platform port-asic

Use the **debug platform port-asic** privileged EXEC command to enable debugging of the port application-specific integrated circuit (ASIC) driver. Use the **no** form of this command to disable debugging.

**debug platform port-asic {interrupt | periodic | read | write}**

**no debug platform port-asic {interrupt | periodic | read | write}**

<b>Syntax Description</b>	
<b>interrupt</b>	Display port-ASIC interrupt-related function debug messages.
<b>periodic</b>	Display port-ASIC periodic-function-call debug messages.
<b>read</b>	Display port-ASIC read debug messages.
<b>write</b>	Display port-ASIC write debug messages.

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	
<b>Usage Guidelines</b>	The <b>undebug platform port-asic</b> command is the same as the <b>no debug platform port-asic</b> command.

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

# debug platform port-security

Use the **debug platform port-security** privileged EXEC command to enable debugging of platform-dependent port-security information. Use the **no** form of this command to disable debugging.

**debug platform port-security {add | aging | all | delete | errors | rpc | warnings}**

**no debug platform port-security {add | aging | all | delete | errors | rpc | warnings}**

Syntax Description	<b>add</b> Display secure address addition debug messages. <b>aging</b> Display secure address aging debug messages. <b>all</b> Display all port-security debug messages. <b>delete</b> Display secure address deletion debug messages. <b>errors</b> Display port-security error debug messages. <b>rpc</b> Display remote procedure call (RPC) debug messages. <b>warnings</b> Display warning debug messages.
--------------------	--

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

**Usage Guidelines** The **udebug platform port-security** command is the same as the **no debug platform port-security** command.

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

---

 debug platform qos-acl-tcam

# debug platform qos-acl-tcam

Use the **debug platform qos-acl-tcam** privileged EXEC command to enable debugging of the quality of service (QoS) and access control list (ACL) ternary content addressable memory (TCAM) manager software. Use the **no** form of this command to disable debugging.

**debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}**

**no debug platform qos-acl-tcam {all | ctcam | errors | labels | mask | rpc | tcam}**

<b>Syntax Description</b>	
<b>all</b>	Display all QoS and ACL TCAM (QATM) manager debug messages.
<b>ctcam</b>	Display Cisco TCAM (CTCAM) related-events debug messages.
<b>errors</b>	Display QATM error-related-events debug messages.
<b>labels</b>	Display QATM label-related-events debug messages.
<b>mask</b>	Display QATM mask-related-events debug messages.
<b>rpc</b>	Display QATM remote procedure call (RPC) related-events debug messages.
<b>tcam</b>	Display QATM TCAM-related events debug messages.

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	
------------------------	--

<b>Usage Guidelines</b>	The <b>undebug platform qos-acl-tcam</b> command is the same as the <b>no debug platform qos-acl-tcam</b> command.
-------------------------	--

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

# debug platform resource-manager

Use the **debug platform resource-manager** privileged EXEC command to enable debugging of the resource manager software. Use the **no** form of this command to disable debugging.

**debug platform resource-manager {all | dm | erd | errors | madmed | sd | stats | vld}**

**no debug platform resource-manager {all | dm | erd | errors | madmed | sd | stats | vld}**

Syntax Description	<b>all</b> Display all resource manager debug messages.
<b>dm</b>	Display destination-map debug messages.
<b>erd</b>	Display equal-cost-route descriptor-table debug messages.
<b>errors</b>	Display error debug messages.
<b>madmed</b>	Display the MAC address descriptor table and multi-expansion descriptor table debug messages.
<b>sd</b>	Display the station descriptor table debug messages.
<b>stats</b>	Display statistics debug messages.
<b>vld</b>	Display the VLAN-list descriptor debug messages.

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

**Usage Guidelines**      The **undebug platform resource-manager** command is the same as the **no debug platform resource-manager** command.

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

---

 debug platform snmp

# debug platform snmp

Use the **debug platform snmp** privileged EXEC command to enable debugging of the platform-dependent Simple Network Management Protocol (SNMP) software. Use the **no** form of this command to disable debugging.

**debug platform snmp**

**no debug platform snmp**

---

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

---

**Defaults** Debugging is disabled.

---

**Command Modes** Privileged EXEC

---

**Command History**

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

---

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

# debug platform span

Use the **debug platform span** privileged EXEC command to enable debugging of the platform-dependent Switched Port Analyzer (SPAN) software. Use the **no** form of this command to disable debugging.

**debug platform span**

**no debug platform span**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

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

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

■ **debug platform supervisor-asic**

# debug platform supervisor-asic

Use the **debug platform supervisor-asic** privileged EXEC command to enable debugging of the supervisor application-specific integrated circuit (ASIC). Use the **no** form of this command to disable debugging.

**debug platform supervisor-asic {all | errors | receive | send}**

**no debug platform supervisor-asic {all | errors | receive | send}**

<b>Syntax Description</b>	<b>all</b> Display all supervisor-ASIC event debug messages. <b>errors</b> Display the supervisor-ASIC error debug messages. <b>receive</b> Display the supervisor-ASIC receive debug messages. <b>send</b> Display the supervisor-ASIC send debug messages.
---------------------------	---

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

**Usage Guidelines**      The **undebug platform supervisor-asic** command is the same as the **no debug platform supervisor-asic** command.

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

# debug platform sw-bridge

Use the **debug platform sw-bridge** privileged EXEC command to enable debugging of the software bridging function. Use the **no** form of this command to disable debugging.

**debug platform sw-bridge {broadcast | control | multicast | packet | unicast}**

**no debug platform sw-bridge {broadcast | control | multicast | packet | unicast}**

Syntax Description	<b>broadcast</b> Display broadcast-data debug messages.
<b>control</b>	Display protocol-packet debug messages.
<b>multicast</b>	Display multicast-data debug messages.
<b>packet</b>	Display sent and received data debug messages.
<b>unicast</b>	Display unicast-data debug messages.

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

**Usage Guidelines**      The **undebug platform sw-bridge** command is the same as the **no debug platform sw-bridge** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

■ debug platform tcam

## debug platform tcam

Use the **debug platform team** privileged EXEC command to enable debugging of ternary content addressable memory (TCAM) access and lookups. Use the **no** form of this command to disable debugging.

```
debug platform tcam {log | read | search | write}
debug platform tcam log l2 {acl {input | output} | local | qos}
debug platform tcam log l3 {acl {input | output} | qos}
debug platform tcam read {reg | ssram | tcam}
debug platform tcam search
debug platform tcam write {forw-ram | reg | tcam}
no debug platform tcam {log | read | search | write}
no debug platform tcam log l2 {acl {input | output} | local | qos}
no debug platform tcam log l3 {acl {input | output} | qos}
no debug platform tcam read {reg | ssram | tcam}
no debug platform tcam search
no debug platform tcam write {forw-ram | reg | tcam}
```

Syntax Description	
<b>log l2 {acl {input   output}   local   qos}</b>	Display Layer 2 field-based CAM look-up type debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>acl {input   output}</b>—Display input or output ACL look-up debug messages.</li> <li>• <b>local</b>—Display local forwarding look-up debug messages.</li> <li>• <b>qos</b>—Display classification and quality of service (QoS) look-up debug messages.</li> </ul>
<b>l3 {acl {input   output}   qos}</b>	Display Layer 3 field-based CAM look-up type debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>acl {input   output}</b>—Display input or output ACL look-up debug messages.</li> <li>• <b>qos</b>—Display classification and quality of service (QoS) look-up debug messages.</li> <li>• </li> </ul>

---

<b>read {reg   ssram   tcam}</b>	Display TCAM-read debug messages. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>reg</b>—Display TCAM-register read debug messages.</li><li>• <b>ssram</b>—Display synchronous static RAM (SSRAM)-read debug messages.</li><li>• <b>tcam</b>—Display TCAM-read debug messages.</li></ul>
<b>search</b>	Display supervisor-initiated TCAM-search results debug messages.
<b>write {forw-ram   reg   team}</b>	Display TCAM-write debug messages. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>forw-ram</b>—Display forwarding-RAM write debug messages.</li><li>• <b>reg</b>—Display TCAM-register write debug messages.</li><li>• <b>team</b>—Display TCAM-write debug messages.</li></ul>

---

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

#### Command History

**Usage Guidelines** The **undebbug platform tcam** command is the same as the **no debug platform tcam** command.

#### Related Commands

---

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

---

■ **debug platform udld**

## debug platform udld

Use the **debug platform udld** privileged EXEC command to enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software. Use the **no** form of this command to disable debugging.

**debug platform udld [all | error | rpc {events | messages}]**

**no debug platform udld [all | error | rpc {events | messages}]**

Syntax Description	<b>all</b> (Optional) Display all UDLD debug messages. <b>error</b> (Optional) Display error condition debug messages. <b>rpc {events   messages}</b> (Optional) Display UDLD remote procedure call (RPC) debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>events</b>—Display UDLD RPC events.</li> <li>• <b>messages</b>—Display UDLD RPC messages.</li> </ul>				
Defaults	Debugging is disabled.				
Command Modes	Privileged EXEC				
Command History					
Usage Guidelines	The <b>undebug platform udld</b> command is the same as the <b>no debug platform udld</b> command.				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td><b>show debugging</b></td><td>Displays information about the types of debugging that are enabled.</td></tr> </tbody> </table>	Command	Description	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
Command	Description				
<b>show debugging</b>	Displays information about the types of debugging that are enabled.				

# debug platform vlan

Use the **debug platform vlan** privileged EXEC command to enable debugging of the VLAN manager software. Use the **no** form of this command to disable debugging.

**debug platform vlan {errors | mvid | rpc}**

**no debug platform vlan {errors | mvid | rpc}**

<b>Syntax Description</b>	<b>errors</b> Display VLAN error debug messages. <b>mvid</b> Display mapped VLAN ID allocations and free debug messages. <b>rpc</b> Display remote procedure call (RPC) debug messages.
---------------------------	---

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

**Usage Guidelines**      The **undebbug platform vlan** command is the same as the **no debug platform vlan** command.

## Related Commands

<b>Command</b>	<b>Description</b>
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

**debug pm**

## debug pm

Use the **debug pm** privileged EXEC command to enable debugging of port manager (PM) activity. The port manager is a state machine that controls all the logical and physical interfaces. All features, such as VLANs, UniDirectional Link Detection (UDLD), and so forth, work with the port manager to provide switch functions. Use the **no** form of this command to disable debugging.

```
debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry | sm | span | split | vlan | vp}
no debug pm {all | assert | card | etherchnl | hatable | messages | port | redundancy | registry | sm | span | split | vlan | vp}
```

### Syntax Description

<b>all</b>	Display all PM debug messages.
<b>assert</b>	Display assert debug messages.
<b>card</b>	Display line-card related-events debug messages.
<b>etherchnl</b>	Display EtherChannel related-events debug messages.
<b>hatable</b>	Display Host Access Table events debug messages.
<b>messages</b>	Display PM debug messages.
<b>port</b>	Display port related-events debug messages.
<b>redundancy</b>	Display redundancy debug messages.
<b>registry</b>	Display PM registry invocation debug messages.
<b>sm</b>	Display state-machine related-events debug messages.
<b>span</b>	Display spanning-tree related-events debug messages.
<b>split</b>	Display split-processor debug messages.
<b>vlan</b>	Display VLAN related-events debug messages.
<b>vp</b>	Display virtual port related-events debug messages.



### Note

Though visible in the command-line help strings, the **scp** and **pvlan** keywords are not supported.

### Defaults

Debugging is disabled.

### Command Modes

Privileged EXEC

---

**Command History****Usage Guidelines** The **undebug pm** command is the same as the **no debug pm** command.

---

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

---

**debug port-security**

# debug port-security

Use the **debug port-security** privileged EXEC command to enable debugging of the allocation and states of the port security subsystem. Use the **no** form of this command to disable debugging.

**debug port-security**

**no debug port-security**

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

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines** The **undebug port-security** command is the same as the **no debug port-security** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show port-security</b>	Displays port-security settings for an interface or for the switch.

# debug qos-manager

Use the **debug qos-manager** privileged EXEC command to enable debugging of the quality of service (QoS) manager software. Use the **no** form of this command to disable debugging.

**debug qos-manager {all | event | verbose}**

**no debug qos-manager {all | event | verbose}**

<b>Syntax Description</b>	<b>all</b> Display all QoS-manager debug messages. <b>event</b> Display QoS-manager related-event debug messages. <b>verbose</b> Display QoS-manager detailed debug messages.
---------------------------	---

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

## Command History

**Usage Guidelines**      The **undebug qos-manager** command is the same as the **no debug qos-manager** command.

## Related Commands

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

■ **debug spanning-tree**

# debug spanning-tree

Use the **debug spanning-tree** privileged EXEC command to enable debugging of spanning-tree activities. Use the **no** form of this command to disable debugging.

```
debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}
```

```
no debug spanning-tree {all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | switch | synchronization | uplinkfast}
```

Syntax Description	
<b>all</b>	Display all spanning-tree debug messages.
<b>backbonefast</b>	Display BackboneFast-event debug messages.
<b>bpdu</b>	Display spanning-tree bridge protocol data unit (BPDU) debug messages.
<b>bpdu-opt</b>	Display optimized BPDU handling debug messages.
<b>config</b>	Display spanning-tree configuration change debug messages.
<b>etherchannel</b>	Display EtherChannel-support debug messages.
<b>events</b>	Display spanning-tree topology event debug messages.
<b>exceptions</b>	Display spanning-tree exception debug messages.
<b>general</b>	Display general spanning-tree activity debug messages.
<b>mstp</b>	Debug Multiple Spanning Tree Protocol events.
<b>pvst+</b>	Display per-VLAN spanning-tree plus (PVST+) event debug messages.
<b>root</b>	Display spanning-tree root-event debug messages.
<b>snmp</b>	Display spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
<b>synchronization</b>	Display the spanning-tree synchronization event debug messages.
<b>switch</b>	Display switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms.
<b>uplinkfast</b>	Display UplinkFast-event debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines** The **undebug spanning-tree** command is the same as the **no debug spanning-tree** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show spanning-tree</b>	Displays spanning-tree state information.

---

■ **debug spanning-tree backbonefast**

# debug spanning-tree backbonefast

Use the **debug spanning-tree backbonefast** privileged EXEC command to enable debugging of spanning-tree BackboneFast events. Use the **no** form of this command to disable debugging.

**debug spanning-tree backbonefast [detail | exceptions]**

**no debug spanning-tree backbonefast [detail | exceptions]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed BackboneFast debug messages. <b>exceptions</b> (Optional) Display spanning-tree BackboneFast-exception debug messages.						
<b>Defaults</b>	Debugging is disabled.						
<b>Command Modes</b>	Privileged EXEC						
<b>Command History</b>							
<b>Usage Guidelines</b>	The <b>undebug spanning-tree backbonefast</b> command is the same as the <b>no debug spanning-tree backbonefast</b> command.						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><b>show debugging</b></td><td>Displays information about the types of debugging that are enabled.</td></tr> <tr> <td><b>show spanning-tree</b></td><td>Displays spanning-tree state information.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<b>show debugging</b>	Displays information about the types of debugging that are enabled.	<b>show spanning-tree</b>	Displays spanning-tree state information.
<b>Command</b>	<b>Description</b>						
<b>show debugging</b>	Displays information about the types of debugging that are enabled.						
<b>show spanning-tree</b>	Displays spanning-tree state information.						

# debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** privileged EXEC command to enable debugging of sent and received spanning-tree bridge protocol data units (BPDUs). Use the **no** form of this command to disable debugging.

**debug spanning-tree bpdu [receive | transmit]**

**no debug spanning-tree bpdu [receive | transmit]**

<b>Syntax Description</b>	<b>receive</b> (Optional) Display the nonoptimized path for received BPDU debug messages. <b>transmit</b> (Optional) Display the nonoptimized path for sent BPDU debug messages.
---------------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

**Usage Guidelines** The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show spanning-tree</b>	Displays spanning-tree state information.

---

 debug spanning-tree bpdu-opt
 

---

## debug spanning-tree bpdu-opt

Use the **debug spanning-tree bpdu-opt** privileged EXEC command to enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling. Use the **no** form of this command to disable debugging.

**debug spanning-tree bpdu-opt [detail | packet]**

**no debug spanning-tree bpdu-opt [detail | packet]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Display detailed optimized BPDU-handling debug messages. <b>packet</b> (Optional) Display packet-level optimized BPDU-handling debug messages.
---------------------------	--

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	
<b>Usage Guidelines</b>	The <b>undebug spanning-tree bpdu-opt</b> command is the same as the <b>no debug spanning-tree bpdu-opt</b> command.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show spanning-tree</b>	Displays spanning-tree state information.

# debug spanning-tree mstp

Use the **debug spanning-tree mstp** privileged EXEC command to enable debugging of the Multiple Spanning Tree Protocol (MSTP) software. Use the **no** form of this command to disable debugging.

```
debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

```
no debug spanning-tree mstp {all | boundary | bpdu-rx | bpdu-tx | errors | flush | init | migration | pm | proposals | region | roles | sanity_check | sync | tc | timers}
```

Syntax Description	
<b>all</b>	Enable all the debugging messages.
<b>boundary</b>	Debug flag changes at these boundaries: <ul style="list-style-type: none"> <li>An multiple spanning-tree (MST) region and a single spanning-tree region running Rapid Spanning Tree Protocol (RSTP)</li> <li>An MST region and a single spanning-tree region running 802.1D</li> <li>An MST region and another MST region with a different configuration</li> </ul>
<b>bpdu-rx</b>	Debug the received MST bridge protocol data units (BPDUs).
<b>bpdu-tx</b>	Debug the sent MST BPDUs.
<b>errors</b>	Debug MSTP errors.
<b>flush</b>	Debug the port flushing mechanism.
<b>init</b>	Debug the initialization of the MSTP data structures.
<b>migration</b>	Debug the protocol migration state machine.
<b>pm</b>	Debug MSTP port manager events.
<b>proposals</b>	Debug handshake messages between the designated switch and the root switch.
<b>region</b>	Debug the region synchronization between the switch processor (SP) and the route processor (RP).
<b>roles</b>	Debug MSTP roles.
<b>sanity_check</b>	Debug the received BPDU sanity check messages.
<b>sync</b>	Debug the port synchronization events.
<b>tc</b>	Debug topology change notification events.
<b>timers</b>	Debug the MSTP timers for start, stop, and expire events.

<b>Defaults</b>	Debugging is disabled.
<b>Command Modes</b>	Privileged EXEC
<b>Command History</b>	
<b>Usage Guidelines</b>	The <b>undebug spanning-tree mstp</b> command is the same as the <b>no debug spanning-tree mstp</b> command.

■ **debug spanning-tree mstp**

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show spanning-tree</b>	Displays spanning-tree state information.

# debug spanning-tree switch

Use the **debug spanning-tree switch** privileged EXEC command to enable debugging of the software interface between the Spanning Tree Protocol (STP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

```
debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode] | uplinkfast}
```

```
no debug spanning-tree switch {all | errors | flush | general | helper | pm | rx {decode | errors | interrupt | process} | state | tx [decode] | uplinkfast}
```

Syntax Description	
<b>all</b>	Display all spanning-tree switch debug messages.
<b>errors</b>	Display debug messages for the interface between the spanning-tree software module and the port manager software module.
<b>flush</b>	Display debug messages for the shim flush operation.
<b>general</b>	Display general event debug messages.
<b>helper</b>	Display spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates.
<b>pm</b>	Display port-manager event debug messages.
<b>rx</b>	Display received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>decode</b>—Display decoded received packets.</li> <li>• <b>errors</b>—Display receive error debug messages.</li> <li>• <b>interrupt</b>—Display interrupt service request (ISR) debug messages.</li> <li>• <b>process</b>—Display process receive BPDU debug messages.</li> </ul>
<b>state</b>	Display spanning-tree port state change debug messages;
<b>tx [decode]</b>	Display sent BPDU handling debug messages. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>decode</b>—(Optional) Display decoded sent packets.</li> </ul>
<b>uplinkfast</b>	Display uplinkfast packet transmission debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

**Command History**

**debug spanning-tree switch**

**Usage Guidelines** The **undebug spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.
<b>show spanning-tree</b>	Displays spanning-tree state information.

# debug spanning-tree uplinkfast

Use the **debug spanning-tree uplinkfast** privileged EXEC command to enable debugging of spanning-tree UplinkFast events. Use the **no** form of this command to disable debugging.

**debug spanning-tree uplinkfast [exceptions]**

**no debug spanning-tree uplinkfast [exceptions]**

<b>Syntax Description</b>	<b>exceptions</b> (Optional) Display spanning-tree UplinkFast-exception debug messages.						
<b>Defaults</b>	Debugging is disabled.						
<b>Command Modes</b>	Privileged EXEC						
<b>Command History</b>							
<b>Usage Guidelines</b>	The <b>undebug spanning-tree uplinkfast</b> command is the same as the <b>no debug spanning-tree uplinkfast</b> command.						
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th><b>Command</b></th><th><b>Description</b></th></tr> </thead> <tbody> <tr> <td><a href="#">show debugging</a></td><td>Displays information about the types of debugging that are enabled.</td></tr> <tr> <td><a href="#">show spanning-tree</a></td><td>Displays spanning-tree state information.</td></tr> </tbody> </table>	<b>Command</b>	<b>Description</b>	<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.	<a href="#">show spanning-tree</a>	Displays spanning-tree state information.
<b>Command</b>	<b>Description</b>						
<a href="#">show debugging</a>	Displays information about the types of debugging that are enabled.						
<a href="#">show spanning-tree</a>	Displays spanning-tree state information.						

**debug sw-vlan**

## debug sw-vlan

Use the **debug sw-vlan** privileged EXEC command to enable debugging of VLAN manager activities. Use the **no** form of this command to disable debugging.

```
debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping | notification | packets | redundancy | registries | vtp}
```

```
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping | notification | packets | redundancy | registries | vtp}
```

<b>Syntax Description</b>	<b>badpmcookies</b> Display debug messages for VLAN manager incidents of bad port manager cookies. <b>cfg-vlan {bootup   cli}</b> Display config-vlan debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>bootup</b>—Display messages when the switch is booting up.</li> <li>• <b>cli</b>—Display messages when the command-line interface (CLI) is in config-vlan mode.</li> </ul>
	<b>events</b> Display debug messages for VLAN manager events.
	<b>ifs</b> See the <a href="#">debug sw-vlan ifs</a> command.
	<b>management</b> Display debug messages for VLAN manager management of internal VLANs.
	<b>mapping</b> Display debug messages for VLAN mapping.
	<b>notification</b> See the <a href="#">debug sw-vlan notification</a> command.
	<b>packets</b> Display debug messages for packet handling and encapsulation processes.
	<b>redundancy</b> Display debug messages for VTP VLAN redundancy.
	<b>registries</b> Display debug messages for VLAN manager registries.
	<b>vtp</b> See the <a href="#">debug sw-vlan vtp</a> command.

**Defaults**      Debugging is disabled.

**Command Modes**      Privileged EXEC

**Command History**

**Usage Guidelines**      The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show debugging</b>	Displays information about the types of debugging that are enabled.

Command	Description
<b>show vlan</b>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.
<b>show vtp</b>	Displays general information about VTP management domain, status, and counters.

**debug sw-vlan ifs**

## debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable debugging of the VLAN manager IOS file system (IFS) error tests. Use the **no** form of this command to disable debugging.

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

<b>Syntax Description</b>	<b>open {read   write}</b>	Display VLAN manager IFS file-open operation debug messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>read</b>—Display VLAN manager IFS file-read operation debug messages.</li> <li>• <b>write</b>—Display VLAN manager IFS file-write operation debug messages.</li> </ul>
	<b>read {1   2   3   4}</b>	Display file-read operation debug messages for the specified error test (1, 2, 3, or 4).
	<b>write</b>	Display file-write operation debug messages.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

### Command History

### Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show vlan</b>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

# debug sw-vlan notification

Use the **debug sw-vlan notification** privileged EXEC command to enable debugging of the activation and deactivation of Inter-Link Switch (ISL) VLAN IDs. Use the **no** form of this command to disable debugging.

```
debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}
```

```
no debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}
```

Syntax Description		
	<b>accfwdchange</b>	Display debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
	<b>allowedvlancfgchange</b>	Display debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
	<b>fwdchange</b>	Display debug messages for VLAN manager notification of spanning-tree forwarding changes.
	<b>linkchange</b>	Display debug messages for VLAN manager notification of interface link-state changes.
	<b>modechange</b>	Display debug messages for VLAN manager notification of interface mode changes.
	<b>pruningcfgchange</b>	Display debug messages for VLAN manager notification of changes to the pruning configuration.
	<b>statechange</b>	Display debug messages for VLAN manager notification of interface state changes.

**Defaults** Debugging is disabled.

**Command Modes** Privileged EXEC

## Command History

**Usage Guidelines** The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show vlan</b>	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

---

```
debug sw-vlan vtp
```

---

## debug sw-vlan vtp

Use the **debug sw-vlan vtp** privileged EXEC command to enable debugging of the VLAN Trunking Protocol (VTP) code. Use the **no** form of this command to disable debugging.

```
debug sw-vlan vtp {events | packets | pruning [packets | xmit] | redundancy | xmit}
```

```
no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}
```

<b>Syntax Description</b>	<b>events</b> Display debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code. <b>packets</b> Display debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the IOS VTP platform-dependent layer, except for pruning packets. <b>pruning [packets   xmit]</b> Display debug messages generated by the pruning segment of the VTP code. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>packets</b>—(Optional) Display debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the IOS VTP platform-dependent layer.</li> <li>• <b>xmit</b>—(Optional) Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the IOS VTP platform-dependent layer to send.</li> </ul>
<b>redundancy</b>	Display debug messages for VTP redundancy.
<b>xmit</b>	Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the IOS VTP platform-dependent layer to send, except for pruning packets.

---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

---

### Command History

**Usage Guidelines** The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no further parameters are entered after the **pruning keyword**, VTP pruning debugging messages appear. They are generated by the VTP\_PRUNING\_LOG\_NOTICE, VTP\_PRUNING\_LOG\_INFO, VTP\_PRUNING\_LOG\_DEBUG, VTP\_PRUNING\_LOG\_ALERT, and VTP\_PRUNING\_LOG\_WARNING macros in the VTP pruning code.

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show vtp</b>	Displays general information about VTP management domain, status, and counters.

**debug udld**

# debug udld

Use the **debug udld** privileged EXEC command to enable debugging of the UniDirectional Link Detection (UDLD) feature. Use the **no** form of this command to disable UDLD debugging.

**debug udld {events | packets | registries}**

**no debug udld {events | packets | registries}**

<b>Syntax Description</b>	<b>events</b> Display debug messages for UDLD process events as they occur. <b>packets</b> Display debug messages for the UDLD process as it receives packets from the packet queue and tries to send them at the request of the UDLD protocol code. <b>registries</b> Display debug messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.
---------------------------	---

<b>Defaults</b>	Debugging is disabled.
-----------------	------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

**Command History**

The **undebug udld** command is the same as the **no debug udld** command.

For **debug udld events**, these debugging messages appear:

- General UDLD program logic flow
- State machine state changes
- Program actions for the set and clear ErrDisable state
- Neighbor cache additions and deletions
- Processing of configuration commands
- Processing of link-up and link-down indications

For **debug udld packets**, these debugging messages appear:

- General packet processing program flow on receipt of an incoming packet
- Indications of the contents of the various pieces of packets received (such as type length versions [TLVs]) as they are examined by the packet reception code
- Packet transmission attempts and the outcome

For **debug udld registries**, these categories of debugging messages appear:

- Sub-block creation
- Fiber-port status changes
- State change indications from the port manager software
- MAC address registry calls

Related Commands	Command	Description
	<b>show debugging</b>	Displays information about the types of debugging that are enabled.
	<b>show udld</b>	Displays UDLD administrative and operational status for all ports or the specified port.

**debug vqpc**

# debug vqpc

Use the **debug vqpc** privileged EXEC command to enable debugging of the VLAN Query Protocol (VQP) client. Use the **no** form of this command to disable debugging.

**debug vqpc [all | cli | events | learn | packet]**

**no debug vqpc [all | cli | events | learn | packet]**

Syntax Description	
<b>all</b>	(Optional) Display all VQP client debug messages.
<b>cli</b>	(Optional) Display the VQP client command-line interface (CLI) debug messages.
<b>events</b>	(Optional) Display VQP client event debug messages.
<b>learn</b>	(Optional) Display VQP client address learning debug messages.
<b>packet</b>	(Optional) Display VQP client packet information debug messages.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History****Usage Guidelines**

The **undebug vqpc** command is the same as the **no debug vqpc** command.

**Related Commands**

Command	Description
<b>show debugging</b>	Displays information about the types of debugging that are enabled.



## APPENDIX

# 1

## Catalyst Switch Show Platform Commands

---

This appendix describes the **show platform** privileged EXEC commands that have been created or changed for use with the Catalyst switch. These commands display information helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

■ show platform acl

## show platform acl

Use the **show platform acl** privileged EXEC command to display platform-dependent access control list (ACL) manager information.

```
show platform acl {interface interface-id | label label-number [detail] | statistics asic-number | usage asic-number [summary] | vlan vlan-id}
```

Syntax Description	<b>interface</b> <i>interface-id</i>	Display per-interface ACL manager information for the specified interface. The interface can be a physical interface or a VLAN.
<b>label</b> <i>label-number</i> [ <b>detail</b> ]		Display per-label ACL manager information. The <i>label-number</i> range is 0 to 255. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>detail</b>—(Optional) Display detailed ACL manager label information.</li> </ul>
<b>statistics</b> <i>asic-number</i>		Display per-ASIC ACL manager information. The <i>asic-number</i> is the port ASIC number, either 0 or 1.
<b>usage</b> <i>asic-number</i> [ <b>summary</b> ]		Display per-ASIC ACL usage information. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>summary</b>—(Optional) Display usage information in a brief format.</li> </ul>
<b>vlan</b> <i>vlan-id</i>		Display per-VLAN ACL manager information. The <i>vlan-id</i> range is from 1 to 4094.

**Command Modes** Privileged EXEC

### Command History

### Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform backup interface

Use the **show platform backup interface** privileged EXEC command to display platform-dependent backup information used in a Flex Links configuration.

**show platform backup interface [interface-id | dummyQ]**

<b>Syntax Description</b>	<i>interface-id</i> (Optional) Display backup information for all interfaces or the specified interface. The interface can be a physical interface or a port channel. <b>dummyQ</b> (Optional) Display dummy queue information.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

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

■ **show platform etherchannel**

## show platform etherchannel

Use the **show platform etherchannel** privileged EXEC command to display platform-dependent EtherChannel information.

**show platform etherchannel {flags | time-stamps}**

<b>Syntax Description</b>	
<b>flags</b>	Display EtherChannel port flags.
<b>time-stamps</b>	Display EtherChannel time stamps.

**Command Modes** Privileged EXEC

**Command History**

**Usage Guidelines**

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform forward

Use the **show platform forward** privileged EXEC command for an interface to specify how the hardware would forward a frame that matches the specified parameters.

```
show platform forward interface-id [vlan vlan-id] src-mac dst-mac [l3protocol-id] [ipv6 | sap | snap] [cos cos] [ip src-ip dst-ip [frag field] [dscp dscp] {l4protocol-id | icmp icmp-type icmp-code | igmp igmp-version igmp-type | sctp src-port dst-port | tcp src-port dst-port flags | udp src-port dst-port}]}
```

Syntax Description	
<i>interface-id</i>	The input physical interface, the port on which the packet comes in to the switch.
<b>vlan</b> <i>vlan-id</i>	(Optional) Input VLAN ID. The range is 1 to 4094. If not specified, and the input interface is not a routed port, the default is 1.
<b>src-mac</b>	48-bit source MAC address.
<b>dst-mac</b>	48-bit destination MAC address.
<b>l3protocol-id</b>	(Optional) The Layer 3 protocol used in the packet. The number is a value 0 to 65535.
<b>ipv6</b>	(Optional) IPv6 frame.
<b>sap</b>	(Optional) Service access point (SAP) encapsulation type.
<b>snap</b>	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type.
<b>cos</b> <i>cos</i>	(Optional) Class of service (CoS) value of the frame. The range is 0 to 7.
<b>ip</b> <i>src-ip dst-ip</i>	(Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation.
<b>frag</b> <i>field</i>	(Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535.
<b>dscp</b> <i>dscp</i>	(Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63.
<b>l4protocol-id</b>	The numeric value of the Layer 4 protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), and 89 is Open Shortest Path First (OSPF). If the protocol is TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or Internet Group Management Protocol (IGMP), you should use the appropriate keyword instead of a numeric value.
<b>icmp</b> <i>icmp-type</i> <i>icmp-code</i>	ICMP parameters. The <i>icmp-type</i> and <i>icmp-code</i> ranges are 0 to 255.
<b>igmp</b> <i>igmp-version</i> <i>igmp-type</i>	IGMP parameters. The <i>igmp-version</i> range is 1 to 15; the <i>igmp-type</i> range is 0 to 15.
<b>sctp</b> <i>src-port dst-port</i>	Stream Control Transmission Protocol (SCTP) parameters. The ranges for the SCTP source and destination ports are 0 to 65535.
<b>tcp</b> <i>src-port dst-port</i> <i>flags</i>	TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte in the header. The <i>src-port</i> and <i>dst-port</i> ranges are 0 to 65535. The flag range is 0 to 1024.
<b>udp</b> <i>src-port dst-port</i>	UDP parameters. The <i>src-port</i> and <i>dst-port</i> ranges are 0 to 65535.

■ **show platform forward**

---

**Command Modes** Privileged EXEC

---

**Command History**

**Usage Guidelines**

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

---

**Examples**

For examples of the **show platform forward** command output displays and what they mean, see the “Troubleshooting” chapter of the software configuration guide for this release.

# show platform frontend-controller

Use the **show platform frontend-controller** privileged EXEC command to display counter and status information for the front-end controller manager and subordinate applications and to display the hardware and software information for the front-end controller.

```
show platform frontend-controller {buffer | generic | manager number | subordinate number | version number}
```

Syntax Description		
	<b>buffer</b>	Display the last 1024 bytes sent from the manager to the subordinate and the reverse.
	<b>generic</b>	Display the generic counters that do not specifically apply to the manager or subordinate.
	<b>manager number</b>	Display the counters for the manager and the subordinate specified by <i>number</i> . See the “Usage Guidelines” section for the <i>number</i> range.
	<b>subordinate number</b>	Display the subordinate status and the counters for the subordinate specified by <i>number</i> . See the “Usage Guidelines” section for the <i>number</i> range.
	<b>version number</b>	Display the hardware and software version information for the subordinate status specified by <i>number</i> . See the “Usage Guidelines” section for the <i>number</i> range.

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.



**Note**

---

■ show platform ip igmp snooping

# show platform ip igmp snooping

Use the **show platform ip igmp snooping** privileged EXEC command to display platform-dependent Internet Group Management Protocol (IGMP) snooping information.

```
show platform ip igmp snooping {all | control [di] | counters | flood [vlan vlan-id] | group  
ip-address | hardware | retry [count | local [count] | remote [count]]}
```

Syntax Description	
<b>all</b>	Display all IGMP snooping platform IP multicast information.
<b>control [di]</b>	Display IGMP snooping control entries. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>di</b>—(Optional) Display IGMP snooping control destination index entries.</li> </ul>
<b>counters</b>	Display IGMP snooping counters.
<b>flood [vlan <i>vlan-id</i>]</b>	Display IGMP snooping flood information. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>vlan <i>vlan-id</i></b>—(Optional) Display flood information for the specified VLAN. The range is 1 to 4094.</li> </ul>
<b>group <i>ip-address</i></b>	Display the IGMP snooping multicast group information, where <i>ip-address</i> is the IP address of the group.
<b>hardware</b>	Display IGMP snooping information loaded into hardware.
<b>retry [count   local [count]]</b>	Display IGMP snooping retry information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>count</b>—(Optional) Display only the retry count.</li> <li>• <b>local</b>—(Optional) Display local retry entries.</li> </ul>
<b>remote [count]</b>	Display remote entries. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>count</b>—(Optional) Display only the remote count.</li> </ul>

---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

## Command History

### Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform ip unicast

Use the **show platform ip unicast** privileged EXEC command to display platform-dependent IP unicast routing information.

```
show platform ip unicast {adjacency | cef-idb | counts | dhcp | failed {adjacency | arp [A.B.C.D] | route} | loadbalance | mpaths | proxy | route | standby | statistics | table | trace}
```

Syntax Description	
<b>adjacency</b>	Display the platform adjacency database.
<b>cef-idb</b>	Display platform information corresponding to Cisco Express Forwarding (CEF) interface descriptor block.
<b>counts</b>	Display the counts for the Layer 3 unicast databases.
<b>dhcp</b>	Display the DHCP system dynamic addresses.
<b>failed {adjacency   arp [A.B.C.D]   route}</b>	Display the hardware resource failures. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>adjacency</b>—Display the adjacency entries that failed to be programmed in hardware.</li> <li>• <b>arp</b>—Display the Address Resolution Protocol (ARP) deletions due to failure and retries.</li> <li>• <b>A.B.C.D</b>—(Optional) Prefix of the ARP entries to display.</li> <li>• <b>route</b>—Display the route entries that were not programmed in hardware.</li> </ul>
<b>loadbalance</b>	Display the platform loadbalance database.
<b>mpaths</b>	Display the Layer 3 unicast routing multipath adjacency database.
<b>proxy</b>	Display the platform proxy ARP database.
<b>route</b>	Display the platform route database.
<b>standby</b>	Display the platform standby information.
<b>statistics</b>	Display the Layer 3 unicast routing accumulated statistics.
<b>table</b>	Display the platform IP version 4 (IPv4) information.
<b>trace</b>	Display the platform event trace logs.

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.



Though visible in the command-line help strings, the **proxy** and **table** keywords are not supported.

■ show platform layer4op

# show platform layer4op

Use the **show platform layer4op** privileged EXEC command to display platform-dependent Layer 4 operator information.

**show platform layer4op {acl | pacl [port-asic] | qos [port-asic]} {and-or | map | or-and | vcu}**

Syntax Description	
<b>acl</b>	Display access control list (ACL) Layer 4 operators information.
<b>pacl [port-asic]</b>	Display port ACL Layer 4 operators information. The keyword has this meaning: <ul style="list-style-type: none"><li>• <i>port-asic</i>—(Optional) Port ASIC number.</li></ul>
<b>qos [port-asic]</b>	Display quality of service (QoS) Layer 4 operators information. The keyword has this meaning: <ul style="list-style-type: none"><li>• <i>port-asic</i>—(Optional) QoS port ASIC number.</li></ul>
<b>and-or</b>	Display AND-OR registers information.
<b>map</b>	Display select map information.
<b>or-and</b>	Display OR-AND registers information.
<b>vcu</b>	Display value compare unit (VCU) register information.

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform mac-address-table

Use the **show platform mac-address-table** privileged EXEC command to display platform-dependent MAC address table information.

```
show platform mac-address-table [aging-array | hash-table | mac-address mac-address] [vlan vlan-id]]
```

Syntax Description	
<b>aging-array</b>	(Optional) Display the MAC address table aging array.
<b>hash-table</b>	(Optional) Display the MAC address table hash table.
<b>mac-address</b> <i>mac-address</i>	(Optional) Display the MAC address table MAC address information, where <i>mac-address</i> is the 48-bit hardware address.
<b>vlan</b> <i>vlan-id</i>	(Optional) Display information for the specified VLAN. The range is 1 to 4094.

**Command Modes** Privileged EXEC

## Command History

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

■ **show platform messaging**

# show platform messaging

Use the **show platform messaging** privileged EXEC command to display platform-dependent application and performance message information.

```
show platform messaging {application [incoming | outgoing | summary] | hiperf [class-number]}
```

---

## Syntax Description

<b>application [incoming   outgoing   summary]</b>	Display application message information. The keywords have these meanings:
	<ul style="list-style-type: none"> <li>• <b>incoming</b>—(Optional) Display only information about incoming application messaging requests.</li> <li>• <b>outgoing</b>—(Optional) Display only information about incoming application messaging requests.</li> <li>• <b>summary</b>—(Optional) Display summary information about all application messaging requests.</li> </ul>
<b>hiperf [class-number]</b>	Display outgoing high-performance message information. Specify the <i>class-number</i> option to display information about high-performance messages for this class number. The range is 0 to 36.

---



---

## Command Modes

Privileged EXEC

---

## Command History

### Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

# show platform monitor

Use the **show platform monitor** privileged EXEC command to display platform-dependent Switched Port Analyzer (SPAN) information.

**show platform monitor [session *session-number*]**

Syntax Description	session <i>session-number</i>	(Optional) Display SPAN information for the specified SPAN session. The range is 1 to 66.
--------------------	----------------------------------	---

Command Modes	Privileged EXEC
---------------	-----------------

## Command History

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

**■ show platform mvr table**

# show platform mvr table

Use the **show platform mvr table** privileged EXEC command to display the platform-dependent Multicast VLAN Registration (MVR) multi-expansion descriptor (MED) group mapping table.

## show platform mvr table

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

**Command Modes** Privileged EXEC

### Command History

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

# show platform pm

Use the **show platform pm** privileged EXEC command to display platform-dependent port-manager information.

```
show platform pm {counters | group-masks | idbs {active-idbs | deleted-idbs} | if-numbers |
link-status | platform-block | port-info interface-id | vlan {info | line-state}}
```

Syntax Description	
<b>counters</b>	Display module counters information.
<b>group-masks</b>	Display EtherChannel group masks information.
<b>idbs {active-idbs   deleted-idbs}</b>	Display interface data block (IDB) information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>active-idbs</b>—Display active IDB information.</li> <li>• <b>deleted-idbs</b>—Display deleted and leaked IDB information.</li> </ul>
<b>if-numbers</b>	Display interface numbers information.
<b>link-status</b>	Display local port link status information.
<b>platform-block</b>	Display platform port block information.
<b>port-info interface-id</b>	Display port administrative and operation fields for the specified interface.
<b>vlan {info   line-state}</b>	Display platform VLAN information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>info</b>—Display information for active VLANs.</li> <li>• <b>line-state</b>—Display line-state information.</li> </ul>

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should 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.

■ show platform port-asic

## show platform port-asic

Use the **show platform port-asic** privileged EXEC command to display platform-dependent port ASIC register information.

```
show platform port-asic {cpu-queue-map-table [asic number | port number [asic number]] |  
dest-map index number |  
etherchannel-info [asic number | port number [asic number]] |  
exception [asic number | port number [asic number]] |  
global-status [asic number | port number [asic number]] |  
learning [asic number | port number [asic number]] |  
mac-info [asic number | port number [asic number]] |  
mvid [asic number] |  
packet-info-ram [asic number | index number [asic number]] |  
port-info [asic number | port number [asic number]] |  
prog-parser [asic number | port number [asic number]] |  
receive {buffer-queue | port-fifo | supervisor-sram} [asic number | port number [asic  
number]] |  
span [vlan-id [asic number] | [asic number]  
stats {drop | enqueue | miscellaneous | supervisor} [asic number | port number [asic  
number]] |  
transmit {port-fifo | queue | supervisor-sram} [asic number | port number [asic number]]  
vct [asic number | port number [asic number]]  
version}
```

---

Syntax Description	
<b>cpu-queue-map-table</b> [asic number   port number [asic number]]	Display the CPU queue-map table entries. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27.</li> </ul>
<b>dest-map index number</b>	Display destination-map information for the specified index. The range is 0 to 65535.
<b>etherchannel-info</b> [asic number   port number [asic number]]	Display the contents of the EtherChannel information register. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>exception</b> [asic number   port number [asic number]]	Display the exception-index register information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>

---

---

<b>global-status [asic number   port number [asic number]]</b>	Display global and interrupt status. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>
<b>learning [asic number   port number [asic number]]</b>	Display entries in the learning cache. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>
<b>mac-info [asic number   port number [asic number]]</b>	Display the contents of the MAC information register. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>
<b>mvid [asic number]</b>	Display the mapped VLAN ID table. The keyword has this meaning: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li></ul>
<b>packet-info-ram [asic number   index number [asic number]]</b>	Display the packet information RAM. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>index number</b>—(Optional) Display information for the specified packet RAM index number and ASIC number. The range is 0 to 63.</li></ul>
<b>port-info [asic number   port number [asic number]]</b>	Display port information register values. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>

---

## show platform port-asic

<b>prog-parser [asic number   port number [asic number]]</b>	Display the programmable parser tables. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>
<b>receive {buffer-queue   port-fifo   supervisor-sram} [asic number   port number [asic number]]</b>	Display receive information. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>buffer-queue</b>—Display the buffer queue information.</li><li>• <b>port-fifo</b>—Display the port-FIFO information.</li><li>• <b>supervisor-sram</b>—Display the supervisor static RAM (SRAM) information.</li><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>
<b>span [vlan-id   asic number]</b>	Display the Switched Port Analyzer (SPAN)-related information. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>vlan-id</b>—(Optional) Display information for the specified VLAN. The range is 0 to 1023.</li><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li></ul>
<b>stats {drop   enqueue   miscellaneous   supervisor} [asic number   port number [asic number]]</b>	Display raw statistics for the port ASIC. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>drop</b>—Display drop statistics.</li><li>• <b>enqueue</b>—Display enqueue statistics.</li><li>• <b>miscellaneous</b>—Display miscellaneous statistics.</li><li>• <b>supervisor</b>—Display supervisor statistics.</li><li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li><li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li></ul>

<b>transmit {port-fifo   queue   supervisor-sram} [asic number   port number [asic number]]</b>	Display transmit information. The keywords have these meanings:
	<ul style="list-style-type: none"> <li>• <b>port-fifo</b>—Display the contents of the port-FIFO information register.</li> <li>• <b>queue</b>—Display the contents of the queue information register.</li> <li>• <b>supervisor-sram</b>—Display supervisor SRAM information.</li> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>vct [asic number   port number [asic number]]</b>	Display the VLAN compression table entries for the specified ASIC or for the specified port and ASIC. The keywords have these meanings:
	<ul style="list-style-type: none"> <li>• <b>asic number</b>—(Optional) Display information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port number</b>—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports.</li> </ul>
<b>version</b>	Display version and device type information for port ASICS.

**Command Modes** Privileged EXEC

#### Command History

#### Usage Guidelines

You should 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.

**■ show platform port-security**

# show platform port-security

Use the **show platform port-security** privileged EXEC command to display platform-dependent port-security information.

**show platform port-security**

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

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should 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.

# show platform qos

Use the **show platform qos** privileged EXEC command to display platform-dependent quality of service (QoS) information.

```
show platform qos {label asic number | policer {parameters asic number | port alloc number asic number}}
```

<b>Syntax Description</b>	<b>label asic number</b> Display QoS label maps for the specified ASIC. (Optional) For <b>asic number</b> , the range is 0 to 1.
	<b>policer {parameters asic number   port alloc number asic number}</b> Display policer information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>parameters asic number</b>—Display parameter information for the specified ASIC. The range is 0 to 1.</li> <li>• <b>port alloc number asic number</b>—Display port allocation information for the specified port and ASIC. The port allocation range is 0 to 25. The ASIC range is 0 to 1.</li> </ul>

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should 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.

■ show platform resource-manager

# show platform resource-manager

Use the **show platform resource-manager** privileged EXEC command to display platform-dependent resource-manager information.

```
show platform resource-manager {dm [index number] | erd [index number] |
    mad [index number] | med [index number] | mod | msm {hash-table [vlan vlan-id] |
    mac-address mac-address [vlan vlan-id]} | sd [index number] |
    vld [index number]}
```

Syntax Description		
	<b>dm [index number]</b>	Display the destination map. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
	<b>erd [index number]</b>	Display the equal-cost-route descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
	<b>mad [index number]</b>	Display the MAC-address descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
	<b>med [index number]</b>	Display the multi-expansion descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
	<b>mod</b>	Display the resource-manager module information.
	<b>msm {hash-table [vlan vlan-id]   mac-address mac-address [vlan vlan-id]}</b>	Display the MAC-address descriptor table and the station descriptor table information. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>hash-table [vlan vlan-id]</b>—Display the hash table for all VLANs or the specified VLAN. The range is 1 to 4094.</li> <li>• <b>mac-address mac-address [vlan vlan-id]</b>—Display the MAC-address descriptor table for the specified MAC address represented by the 48-bit hardware address for all VLANs or the specified VLAN. The range is 1 to 4094.</li> </ul>
	<b>sd [index number]</b>	Display the station descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>
	<b>vld [index number]</b>	Display the VLAN-list descriptor table for the specified index. The keyword has this meaning: <ul style="list-style-type: none"> <li>• <b>index number</b>—(Optional) Display the specified index. The range is 0 to 65535.</li> </ul>

Command Modes

Privileged EXEC

**Command History****Usage Guidelines**

You should 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.

**■ show platform snmp counters**

# show platform snmp counters

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

**show platform snmp counters**

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

**Command Modes** Privileged EXEC

## Command History

### Usage Guidelines

You should 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.

# show platform spanning-tree

Use the **show platform spanning-tree** privileged EXEC command to display platform-dependent spanning-tree information.

**show platform spanning-tree synchronization [detail | vlan *vlan-id*]**

Syntax Description	Display spanning-tree state synchronization information. The keywords have these meanings:
<b>synchronization [detail   vlan <i>vlan-id</i>]</b>	<ul style="list-style-type: none"><li>• <b>detail</b>—(Optional) Display detailed spanning-tree information.</li><li>• <b>vlan <i>vlan-id</i></b>—(Optional) Display VLAN switch spanning-tree information for the specified VLAN. The range is 1 to 4094.</li></ul>

Command Modes	Privileged EXEC
---------------	-----------------

## Command History

Usage Guidelines	You should 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.
------------------	--

■ **show platform stp-instance**

## show platform stp-instance

Use the **show platform stp-instance** privileged EXEC command to display platform-dependent spanning-tree instance information.

**show platform stp-instance *vlan-id***

<b>Syntax Description</b>	<i>vlan-id</i>	Display spanning-tree instance information for the specified VLAN. The range is 1 to 4094.
---------------------------	----------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

### Command History

<b>Usage Guidelines</b>	You should 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.
-------------------------	--

# show platform tcam

Use the **show platform team** privileged EXEC command to display platform-dependent ternary content addressable memory (TCAM) driver information.

```
show platform team {errors | handle number | log-results | table {acl | all | local | mac-address |
    qos | station | vlan-list} | usage} [asic number [detail [invalid]] | [index number [detail
    [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail
    [invalid]] | invalid]]
show platform team table acl [asic number [detail [invalid]] | [index number [detail [invalid]] |
    invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] |
    invalid]]
show platform team table all [asic number [detail [invalid]] | [index number [detail [invalid]] |
    invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] |
    invalid]]
show platform team table local [asic number [detail [invalid]] | [index number [detail [invalid]] |
    invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] |
    invalid]]
show platform team table mac-address [asic number [detail [invalid]] | [index number [detail
    [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail
    [invalid]] | invalid]]
show platform team table qos [asic number [detail [invalid]] | [index number [detail [invalid]] |
    invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail [invalid]] |
    invalid]]
show platform team table station [asic number [detail [invalid]] | [index number [detail
    [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail
    [invalid]] | invalid]]
show platform team table vlan-list [ [asic number [detail [invalid]] | [index number [detail
    [invalid]] | invalid | num number [detail [invalid]] | invalid] | [invalid] | [num number [detail
    [invalid]] | invalid]]]
```

Syntax Description		
	<b>errors</b>	Displays TCAM memory consistency check errors in the Hulc Quality of Service (QoS)/access control list (ACL) TCAM Manager (HQATM), Hulc Forwarding TCAM Manager (HFTM), and unassigned spaces on the TCAM.
	<b>handle number</b>	Display the TCAM handle. The range is 0 to 4294967295.
	<b>log-results</b>	Display the TCAM log results.

---

■ show platform tcam

---

<b>table {acl   all   local   mac-address   qos   station   vlan-list}</b>	Display lookup and forwarding table information. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>acl</b>—Display the access-control list (ACL) table.</li><li>• <b>all</b>—Display all the TCAM tables.</li><li>• <b>local</b>—Display the local table.</li><li>• <b>mac-address</b>—Display the MAC-address table.</li><li>• <b>qos</b>—Display the QoS table.</li><li>• <b>station</b>—Display the station table.</li><li>• <b>vlan-list</b>—Display the VLAN list table.</li></ul>
<b>usage</b>	Display the CAM and forwarding table usage.
<b>[[asic number [detail [invalid]]   [index number [detail [invalid]]]   invalid   num number [detail [invalid]]   invalid]   [invalid]   [invalid]   [num number [detail [invalid]]]   invalid]]</b>	Display information. The keywords have these meanings: <ul style="list-style-type: none"><li>• <b>asic number</b>—Display information for the specified ASIC device ID. The range is 0 to 15.</li><li>• <b>detail [invalid]</b>—(Optional) Display valid or invalid details.</li><li>• <b>index number</b>—(Optional) Display information for the specified TCAM table index. The range is 0 to 32768.</li><li>• <b>num number</b>—(Optional) Display information for the specified TCAM table number. The range is 0 to 32768.</li></ul>

---

**Command Modes** Privileged EXEC

---

Command History	Release	Modification
	12.2(55)SE	Support for the <b>errors</b> keyword was added.

---

**Usage Guidelines** You should 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.

# show platform vlan

Use the **show platform vlan** privileged EXEC command to display platform-dependent VLAN information.

**show platform vlan { misc | mvid | prune | refcount | rpc { receive | transmit } }**

Syntax Description	
<b>misc</b>	Display miscellaneous VLAN module information.
<b>mvid</b>	Display the mapped VLAN ID (MVID) allocation information.
<b>prune</b>	Display the pruning database.
<b>refcount</b>	Display the VLAN lock module-wise reference counts.
<b>rpc { receive   transmit }</b>	Display remote procedure call (RPC) messages. The keywords have these meanings: <ul style="list-style-type: none"> <li>• <b>receive</b>—Display received information.</li> <li>• <b>transmit</b>—Display sent information.</li> </ul>

**Command Modes** Privileged EXEC

## Command History

## Usage Guidelines

You should 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.



## APPENDIX

# 1

## Acknowledgments for Open-Source Software

---

The Cisco IOS software pipe command uses Henry Spencer's regular expression library (regex). The most recent version of the library has been modified slightly in the Catalyst operating system software to maintain compatibility with earlier versions of the library.

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.