Catalyst 3550 Multilayer Switch Command Reference

Cisco IOS Release 12.2(25)SEE
February 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-8566-01

Preface

Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Catalyst 3550 switch, hereafter referred to as *the switch* or the *multilayer switch*. Before using this guide, you should have experience working with the Cisco IOS and the switch software features. Before using this guide, you should have experience working with the Cisco IOS and be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

The Catalyst 3550 switch is supported by either the IP base image (formerly known as the standard multilayer image [SMI]) or the IP services image (formerly known as the enhanced multilayer image [EMI]). The IP services image provides a richer set of enterprise-class features, including hardware-based IP unicast and multicast routing, inter-VLAN routing, routed access control lists (ACLs), and the Hot Standby Router Protocol (HSRP). All Catalyst 3550 Gigabit Ethernet switches are shipped with the IP services image pre-installed. Catalyst 3550 Fast Ethernet switches are shipped with either the IP base image or the IP services image pre-installed. After initial deployment, you can order the upgrade kit to upgrade Catalyst 3550 Fast Ethernet switches from the IP base image to the IP services image.

This guide provides the information you need about the Layer 2 and Layer 3 commands that have been created or changed for use with the Catalyst 3550 family of switches. For information about the standard Cisco IOS Release 12.2 commands, see the Cisco IOS documentation set available from the Cisco.com home page by selecting **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.2** from the Cisco IOS Software drop-down list.

This guide does not provide procedures for configuring your switch. For detailed configuration procedures, see the C*atalyst 3550 Multilayer Switch Software Configuration Guide* for this release.

This guide does not describe system messages you might encounter. For more information, see the *Catalyst 3550 Multilayer Switch 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.

Timesaver Means the following *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Related Publications

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

http://www.cisco.com/en/US/products/hw/switches/ps646/tsd_products_support_series_home.html

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com site and from the telephone numbers listed in the "Obtaining Documentation" section on page xix.

- *Release Notes for the Catalyst 3550 Multilayer Switch* (not orderable but available on Cisco.com)

Note Switch requirements and procedures for initial configurations and software upgrades tend to change and therefore appear only in the release notes. Before installing, configuring, or upgrading the switch, see the release notes on Cisco.com for the latest information.

- *Catalyst 3550 Multilayer Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 3550 Multilayer Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- Device manager online help (available on the switch)
- *Catalyst 3550 Multilayer Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3550 Multilayer Switch Getting Started Guide* (order number DOC-7816575=)
- *Regulatory Compliance and Safety Information for the Catalyst 3550 Multilayer* (order number DOC-7816655=)
- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *1000BASE-T Gigabit Interface Converter Installation Note* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)
- For information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Using the Command-Line Interface

The Catalyst 3550 multilayer switches are 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 2, "Catalyst 3550 Switch Cisco IOS Commands." For information on the boot loader commands, see Appendix A, "Catalyst 3550 Switch Boot Loader Commands." For information on the debug commands, see the Appendix B, "Catalyst 3550 Switch Debug 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. For information on accessing the CLI through the switch console port or through a Telnet session, see the hardware installation guide or the getting started guide.

In this document, IP refers to IP version 4 (IPv4). Layer 3 IP version 6 (IPv6) packets are treated as non-IP packets.

Type of Memory

The switch flash memory stores the Cisco IOS software image, the startup configuration file, and helper files.

Platforms

This IOS release runs on a variety of switches and modules. For a complete list, see the release notes for this switch.

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
- Config-vlan
- 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 **logout** command. To enter privileged EXEC mode, enter the **enable** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Switch#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure** command.
Global configuration	From privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. To enter interface configuration mode, enter the **interface** configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the **interface** command.	`Switch(config-if)#`	To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. To exit to global configuration mode, enter the **exit** command.
Config-vlan	In global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.
VLAN configuration	From privileged EXEC mode, enter the **vlan database** command.	`Switch(vlan)#`	To exit to privileged EXEC mode, enter the **exit** command.
Line configuration	From global configuration mode, specify a line by entering the **line** command.	`Switch(config-line)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

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 view 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 view 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 view 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 view 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**.

config-vlan 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 view 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.

VLAN Configuration Mode

You can use the VLAN configuration commands to create or modify VLAN parameters for VLAN IDs 1 to 1005.

Enter the **vlan database** privileged EXEC command to access VLAN configuration mode:

```
Switch# vlan database
Switch(vlan)#
```

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

```
Switch(vlan)# ?
```

To return to privileged EXEC mode, enter the **abort** VLAN configuration command to abandon the proposed database. Otherwise, enter **exit** to implement the proposed new VLAN database and to return to privileged EXEC mode. When you enter exit or apply, the configuration is saved in the VLAN database; configuration from VLAN configuration mode cannot be saved in the switch configuration file.

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 view 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**.

Catalyst 3550 Switch 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

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Use the accounting methods that follow as the default list for accounting services.
start-stop	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.
broadcast	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.
group	Specify the server group to be used for accounting services. These are valid server group names: • *name*—Name of a server group. • **radius**—List of all RADIUS hosts. • **tacacs+**—List of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enable RADIUS authorization.
tacacs+	(Optional) Enable TACACS+ accounting.

Defaults

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(20)SE	This command was introduced.

Usage Guidelines

This command requires access to a RADIUS server.

Note 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:

```
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)#
```

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

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1x authentication.
dot1x re-authentication	Enables or disables periodic reauthentication.
dot1x timeout reauth-period	Sets the number of seconds between re-authentication attempts.

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 IEEE 802.1x authentication. Use the **no** form of this command to disable authentication.

aaa authentication dot1x {**default**} *method1*

no aaa authentication dot1x {**default**}

Syntax Description

default	Use the listed authentication method that follows this argument as the default method when a user logs in.
method1	Enter the **group radius** keywords to use the list of all RADIUS servers for authentication.

Note Though other commands 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

Release	Modification
12.1(8)EA1	This command was introduced.

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
aaa new-model	Enables the AAA access control model. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Authentication, Authorization, and Accounting > Authentication Commands**.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

aaa authorization network

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

aaa authorization network default group radius

no aaa authorization network default

Syntax Description

default group radius	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

Release	Modification
12.2(25)SEE	This command was introduced.

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 per-user ACLs or 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.

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

access-list hardware program nonblocking

Use the **access-list hardware program nonblocking** global configuration command to cause the system to continue to forward frames even while a new security access-control list (ACL) configuration is being programmed into the hardware. Use the **no** form of this command to return to the default behavior, where traffic is blocked on affected interfaces when changes are made to the security ACL configuration while the hardware is updated with the new configuration.

access-list hardware program nonblocking

no access-list hardware program nonblocking

Syntax Description

This command has no arguments or keywords.

Defaults

Traffic is blocked on affected interfaces while a new ACL configuration is loaded into hardware.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

Usage Guidelines

By default, when changes are made to the configuration of security ACLs, the system completely blocks traffic on the affected ports or VLANs while it is updating the hardware to the new configuration. This includes any changes that affect the ternary content addressable memory (TCAM), including applying an ACL to an interface or making changes to VLAN maps or ACLs that are used for security features. This prevents the possibility of forwarding frames that should have been dropped because a partially loaded configuration permitted a frame that the complete configuration would have blocked.

You can use the **access-list hardware program nonblocking** command to set the system to continue to forward frames while a new security ACL configuration is being programmed into the hardware. Enabling this setting might cause less disruption to traffic that should be allowed while the hardware is being updated, but might also temporarily allow some traffic that would be denied when the new configuration is completely loaded.

Examples

This example shows how to set the system to continue forwarding frames while a new security ACL configuration is being programmed into hardware:

```
Switch (config)# access-list hardware program nonblocking
```

You can verify your setting by entering the **show running-config | include access-list hardware** privileged EXEC command.

Related Commands

Command	Description
access-list {**deny** | **permit**}	Configures a standard numbered ACL. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
action (access map configuration)	Defines or modifies the action for the VLAN access map entry.
ip access-group	Applies an IP access list to a Layer 2 or Layer 3 interface.
ip access-list	Configures a named access list. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
mac access-group	Applies a MAC access list to a Layer 2 interface.
match (access-map configuration)	Defines the match conditions for a VLAN map.
show running-config | include access-list hardware	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
vlan access-map	Creates a VLAN access map or enters access-map configuration mode.
vlan filter	Applies a VLAN map to one or more VLANs.

action

Use the **action** access map configuration command to set the action for the VLAN access map entry. Use the **no** form of this command to return to the default setting.

action {**drop** | **forward**}

no action

Syntax Description

drop	Drop the packet when the specified conditions are matched.
forward	Forward the packet when the specified conditions are matched.

Defaults

The default action is to forward packets.

Command Modes

Access-map configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

In access map configuration mode, use the **match** access map configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

Examples

This example shows how to identify and apply a VLAN access map *vmap4* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list *al2*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

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

Related Commands

Command	Description
access-list {**deny** | **permit**}	Configures a standard numbered ACL. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
ip access-list	Creates a named access list. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
mac access-list extended	Creates a named MAC address access list.
match (access-map configuration)	Defines the match conditions for a VLAN map.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Creates a VLAN access map.

archive download-sw

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

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

Syntax Description

/force-reload	Unconditionally force a system reload after successfully downloading the software image.
/imageonly	Download only the software image but not the HTML files associated with the device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
/leave-old-sw	Keep the old software version after a successful download.
/no-set-boot	Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
/overwrite	Overwrite the software image in flash with the downloaded one.
/reload	Reload the system after successfully downloading the image unless the configuration has been changed and not been saved.
/safe	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.
source-url	The source URL alias for a local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name***.tar** • The syntax for an HTTP server: **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar** • The syntax for a secure HTTP server: **https://**[[*username***:***password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[*//username***@***location*]*/directory*]*/image-name***.tar** • The syntax for the TFTP: **tftp:**[[*//location*]*/directory*]*/image-name***.tar** The *image-name***.tar** is the software image to download and install on the switch.

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

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(25)SE	The **http** and **https** keywords were added.

Usage Guidelines

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

If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

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.

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 space.

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 2-70.

If you leave the existing software in place before downloading the new image, an error results if the existing software will prevent the new image from fitting onto flash memory.

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 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 /image-only 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
archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.
archive upload-sw	Uploads an existing image on the switch to a server.
delete	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-ur*l} | {/**xtract** *source-url* **flash:**/*file-url* [*dir*/*file...*]}

Syntax Description

/**create** *destination-url* **flash:**/*file-url*	Create a new tar file on the local or network file system. For *destination-url*, 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: • The syntax for the local flash filesystem: **flash:** • The syntax for the FTP: **ftp:**[[//*username*[**:***password*]**@***location*]/*directory*]/*tar-filename***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[//*username***@***location*]/*directory*]/*tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[//*location*]/*directory*]/*tar-filename***.tar** The *tar-filename***.tar** is the tar file to be created. For **flash:**/*file-url*, specify the location on the local flash file system from which the new tar file is created. 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.

/table *source-url*	Display the contents of an existing tar file to the screen. For *source-url*, specify the source URL alias for the local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[*//username***@***location*]*/directory*]*/tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[*//location*]*/directory*]*/tar-filename***.tar** The *tar-filename***.tar** is the tar file to display.
/xtract *source-url* **flash:***/file-url* [*dir/file...*]	Extract files from a tar file to the local file system. For *source-url*, specify the source URL alias for the local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/tar-filename***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[*//username***@***location*]*/directory*]*/tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[*//location*]*/directory*]*/tar-filename***.tar** The *tar-filename***.tar** is the tar file from which to extract. For **flash:***/file-url*, specify the location on the local flash file system into which the tar file is extracted. For **flash:***/file-url* [*dir/file...*], specify the location on the local flash file system into which the tar file is extracted. Use the *dir/file...* 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.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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 *c3550-ipservices-tar.122-25.tar* file that is in flash memory. The contents of the tar file appear on the screen:

```
Switch# archive tar /table flash:c3550-ipservices-tar.122-25.tar
info (219 bytes)
c3550-ipservices-mz.122-25.SEB/ (directory)
c3550-ipservices-mz.122-25/html/ (directory)
c3550-ipservices-mz.122-25/c3550-mz.122-25.SEB.bin (6074880 bytes)
c3550-ipservices-mz.122-25/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c3550-ipservices-mz.122-25.SEB/html* directory and its contents:

```
Switch# archive tar /table flash:c3550-ipservices-tar.122-25.SEB.tar
c3550-ipservices-mz.122-25.SEB/html
c3550-ipservices-mz.122-25.SEB/html/ (directory)
c3550-ipservices-mz.122-25SEB/html/const.htm (556 bytes)
c3550-ipservices-mz.122-25SEB/html/xhome.htm (9373 bytes)
c3550-ipservices-mz.122-25SEB/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

Command	Description
archive download-sw	Downloads a new image to the switch.
archive upload-sw	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*

Syntax Description

/version *version_string*	(Optional) Specify the specify version string of the image to be uploaded.
destination-url	The destination URL alias for a local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[*//username*[**:***password*]**@***location*]*/directory*]*/image-name***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[*//username***@***location*]*/directory*]*/image-name***.tar** • The syntax for the TFTP: **tftp:**[[*//location*]*/directory*]*/image-name***.tar** The *image-name***.tar** is the name of the software image to be stored on the server.

Defaults

Uploads the currently running image from the flash: file system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The upload feature is available only if the HTML files associated with the device manager have been installed with the existing image.

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

Image names are case sensitive.

Examples

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

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

Related Commands

Command	Description
archive download-sw	Downloads a new image to the switch.
archive tar	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*

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

acl-name	Name of the ACL.

Defaults

No ARP access lists are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

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 2-74.
- **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 2-269.

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
```

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

Related Commands

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

auto qos voip

Use the **auto qos voip** interface configuration command to automatically configure quality of service (auto-QoS) for voice over IP (VoIP) within a QoS domain. Use the **no** form of this command to change the auto-QoS configuration settings to the standard QoS defaults.

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

no auto qos voip

Syntax Description

cisco-phone	Identify this interface 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.
cisco-softphone	Identify this port as connected to a device running the Cisco SoftPhone, and automatically configure QoS for VoIP.
trust	Identify this interface as connected to a trusted switch or router, and automatically configure QoS for VoIP. The QoS labels of incoming packets are trusted.

Defaults

Auto-QoS is disabled on all interfaces.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic and class of service (CoS) packet labels and to configure the egress queues as summarized in Table 2-1.

Table 2-1 Traffic Types, Packet Labels, and Egress Queues

	VoIP Data Traffic	VoIP Control Traffic	Routing Protocol Traffic	STP[1] BPDU[2] Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP[3]	46	24, 26	48	56	34	—	
CoS	5	3	6	7	4	—	
CoS-to-Queue Map	5	3, 6, 7			4	2	0, 1
Egress Queue	Expedite (queue 4)	70% WRR[4] (queue 3)			20% WRR (queue 2)	20% WRR (queue 2)	10% WRR (queue 1)

1. STP = Spanning Tree Protocol
2. BPDU = bridge protocol data unit
3. DSCP = Differentiated Services Code Point
4. WRR = weighted round robin

Table 2-2 lists the auto-QoS configuration for the egress queues.

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

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight	Queue Size for Gigabit-Capable Ports	Queue Size (in packets) for 10/100 Ethernet Ports
Expedite	4	5	–	10 percent	34 (10 percent)
70% WRR	3	3, 6, 7	70 percent	15 percent	51 (15 percent)
20% WRR	2	2, 4	20 percent	25 percent	82 (25 percent)
10% WRR	1	0, 1	10 percent	50 percent	170 (50 percent)

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.
12.1(20)EA2	The **cisco-softphone** keyword was added, and the generated auto-QoS configuration changed.

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 the edge devices that can classify incoming traffic for QoS.

In releases earlier than Cisco IOS Release 12.1(20)EA2, auto-QoS configures the switch only for VoIP with Cisco IP Phones on switch ports.

In Cisco IOS Release 12.1(20)EA2 or later, 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.

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 interface, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command).
- 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 interface is set to trust the QoS label received in the packet. When a Cisco IP Phone is absent, the ingress classification is set to not trust the QoS label in the packet. The egress queues on the interface are also reconfigured (see Table 2-2).
- 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 egress queues on the interface are also reconfigured (see Table 2-2).
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the interior of the network, the ingress classification on the interface is set to trust the QoS label received in the packet, and the egress queues on the interface are reconfigured (see Table 2-2).

You can enable auto-QoS on static, dynamic-access, 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 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 an interface, use the **no auto qos voip** interface configuration command. When you enter this command, the switch enables standard QoS and changes the auto-QoS settings to the standard-QoS default settings for that interface.

To disable auto-QoS on the switch, use the **no mls qos** global configuration command. When you enter this command, the switch disables QoS on all interfaces and enables pass-through mode.

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 an interface is a trusted device:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip trust
```

This example shows how to enable auto-QoS and to trust the QoS labels received in incoming packets when the device connected to an interface is detected as a Cisco IP Phone:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# auto qos voip cisco-phone
```

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 fastethernet0/1
Switch(config-if)# auto qos voip trust
Switch(config-if)#
4d22h:mls qos map cos-dscp 0 8 16 26 32 46 48 56
4d22h:mls qos min-reserve 5 170
4d22h:mls qos min-reserve 6 85
4d22h:mls qos min-reserve 7 51
4d22h:mls qos min-reserve 8 34
4d22h:mls qos
4d22h:interface FastEthernet0/1
4d22h: mls qos trust cos
4d22h: wrr-queue bandwidth 10 20 70 1
4d22h: wrr-queue min-reserve 1 5
4d22h: wrr-queue min-reserve 2 6
4d22h: wrr-queue min-reserve 3 7
4d22h: wrr-queue min-reserve 4 8
4d22h: no wrr-queue cos-map
4d22h: wrr-queue cos-map 1 0 1
4d22h: wrr-queue cos-map 2 2 4
4d22h: wrr-queue cos-map 3 3 6 7
4d22h: wrr-queue cos-map 4 5
4d22h: priority-queue out
Switchconfig-if)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)#
4d22h:interface GigabitEthernet0/1
4d22h: mls qos trust device cisco-phone
4d22h: mls qos trust cos
4d22h: wrr-queue bandwidth 10 20 70 1
4d22h: wrr-queue queue-limit 50 25 15 10
4d22h: no wrr-queue cos-map
4d22h: wrr-queue cos-map 1 0 1
4d22h: wrr-queue cos-map 2 2 4
4d22h: wrr-queue cos-map 3 3 6 7
4d22h: wrr-queue cos-map 4 5
4d22h: priority-queue out
Switch(config-if)#
```

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

Related Commands

Command	Description
debug auto qos	Enables debugging of the auto-QoS feature.
mls qos map {**cos-dscp** *dscp1 ... dscp8* | **dscp-cos** *dscp-list* **to** *cos*}	Defines the CoS-to-DSCP map or the DSCP-to-CoS map.
mls qos trust	Configures the port trust state.
show auto qos	Displays auto-QoS information.
show mls qos	Displays global QoS configuration information.
show mls qos interface	Displays QoS information at the interface level.
show mls qos maps	Displays QoS mapping information.

boot boothlpr

Use the **boot boothlpr** global configuration command to load a special Cisco IOS image, which when loaded into memory, can load a second Cisco IOS image into memory and launch it. This variable is used only for internal development and testing. Use the **no** form of this command to return to the default setting.

boot boothlpr *filesystem***:***/file-url*

no boot boothlpr

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	The path (directory) and name of a bootable helper image.

Defaults

No helper image is loaded.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the BOOTHLPR environment variable. For more information, see Appendix A, "Catalyst 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot buffersize

Use the **boot buffersize** global configuration command to specify the size of the file system-simulated NVRAM in flash memory. The buffer holds a copy of the configuration file in memory. Use the **no** form of this command to return to the default setting.

boot buffersize *size*

no boot buffersize

Syntax Description

size	The buffer allocation size in bytes. The range is 4096 to 524288 bytes.

Defaults

The default is 32 KB.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The configuration file cannot be larger than the buffer size allocation.

You must reload the switch by using the **reload** privileged EXEC command for this command to take effect.

This command changes the setting of the CONFIG_BUFSIZE environment variable. For more information, see Appendix A, "Catalyst 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	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

Syntax Description

flash:/*file-url*	The path (directory) and name of the configuration file.

Defaults

The default configuration file is flash:config.text.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the CONFIG_FILE environment variable. For more information, see Appendix A, "Catalyst 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	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

Release	Modification
12.1(4)EA1	This command was introduced.

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 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	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 setting.

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

no boot helper

Syntax Description

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

Defaults

No helper files are loaded.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER environment variable. For more information, see Appendix A, "Catalyst 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	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. This variable is used only for internal development and testing. 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

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	The path (directory) and helper configuration file to load.

Defaults

No helper configuration file is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	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

Release	Modification
12.1(4)EA1	This command was introduced.

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 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 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

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

Syntax Description

filename	The name of the private configuration file.

Defaults

The default configuration file is *private-config.text*.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

Usage Guidelines

Only the Cisco IOS software can read and write a copy of the private configuration file. You cannot read, write, delete, or display a copy of this file.

Filenames are case sensitive.

Examples

This example shows how to specify the name of the private configuration file to be *pconfig*:

```
Switch(config)# boot private-config-file pconfig
```

Related Commands

Command	Description
show boot	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

Syntax Description

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

Defaults

The switch attempts to automatically boot 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

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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 3550 Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

channel-group

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

channel-group-number	Specify the channel group number. The range is 1 to 64.
mode	Specify the EtherChannel Port Aggregation Protocol (PAgP) mode of the interface.
active	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.
auto	Enable PAgP only if a PAgP device is detected. Auto mode places an interface into a passive negotiating state, in which the interface 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 **auto** is enabled, silent operation is the default.
desirable	Unconditionally enable PAgP. Desirable mode places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode. When **desirable** is enabled, silent operation is the default.
non-silent	(Optional) Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device.

on	Enable **on** mode. In **on** mode, a usable EtherChannel exists only when both connected port groups are in the **on** mode.
passive	Enable LACP only if a LACP device is detected. Passive mode places an interface into a negotiating state in which the interface responds to LACP packets it receives 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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(12c)EA1	The **active** and **passive** keywords were added.

Usage Guidelines

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but we highly recommend that you do so.

For Layer 2 EtherChannels, you must configure the **channel-group** interface configuration command, which automatically creates the port-channel logical interface. You cannot put Layer 2 interfaces into a manually created port-channel interface.

You create Layer 3 port channels by using the **interface port-channel** command. You must manually configure the port-channel logical interface before putting the interface into the channel group.

Any configuration or attribute changes you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel, but are part of the channel group).

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 interface to a channel group, and to use the interface for transmission. Both ends of the link cannot be set to silent.

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

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

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.

Note If IEEE 802.1x authentication is enabled on a not-yet active port of an EtherChannel in software releases earlier than Cisco IOS Release 12.2(25)SE, the port does not join the EtherChannel.

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

Caution Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Do not assign bridge groups on the physical EtherChannel interfaces because it creates loops.

Examples

This example shows how to assign two interfaces as static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/4 -5
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 set an EtherChannel into PAgP mode:

```
Switch(config-if)# channel-group 1 mode auto
Creating a port-channel interface Port-channel 1
```

This example shows how to set an EtherChannel into LACP mode:

```
Switch(config-if)# channel-group 1 mode passive
Creating a port-channel interface Port-channel 1
```

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

Related Commands

Command	Description
interface port-channel	Accesses or creates the port channel.
show lacp	Display LACP information.

Command	Description
show pagp	Display PAgP information.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

channel-protocol

Use the **channel-protocol** interface configuration command to configure an EtherChannel for the Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP). Use the **no** form of this command to disable PAgP or LACP on the EtherChannel.

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

no channel-protocol

Syntax Description

lacp	Configure an EtherChannel with the LACP protocol.
pagp	Configure an EtherChannel with the PAgP protocol.

Defaults

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP.

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

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

Caution Do not enable Layer 3 addresses on the physical EtherChannel interfaces. To prevent loops, do not assign bridge groups on the physical EtherChannel interfaces.

Examples

This example shows how to set an EtherChannel into PAgP mode:

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

This example shows how to set an EtherChannel into LACP mode:

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

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

Related Commands

Command	Description
show lacp	Display LACP information.
show pagp	Display PAgP information.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

class

Use the **class** policy-map configuration command to define a traffic classification for the policy to act on. Use the **no** form of this command to delete an existing class map.

class *class-map-name*

no class *class-map-name*

Syntax Description

class-map-name	Name of the class map.

Note Though visible in the command-line help strings, the **class** *class-default* option is not supported.

Defaults

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **access-group**, **any**, **dscp**, **destination-address, input-interface**, **precedence**, **protocol**, and **source-address** keywords were removed.

Usage Guidelines

Use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode before you use the **class** command. After you specify 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 an interface by using the **service-policy** interface configuration command.

The class name that you specify in the policy map ties the characteristics for that class to the class map and its match criteria as configured by using the **class-map** global configuration command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

After you enter the **class** command, the switch enters 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.

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 DSCP to 10, and polices the traffic at an average rate of 1 Mbps and for 20 KB bursts. Traffic exceeding the profile is marked down to a DSCP value obtained 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
```

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to the class whose 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

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

Defaults

No class maps are defined.

When neither the **match-all** or **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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-interface 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 in use, this message appears:

```
A class-map with this name already exists
```

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.

To define packet classification on a per-port per-VLAN basis, you must use the **match-all** keyword with the **class-map** global configuration command. You also must enter the **match vlan** *vlan-list* and the **match class-map** *class-map-name* class-map configuration commands. For more information, see the "match (class-map configuration)" section on page 2-226.

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*. *class1* has one match criterion, which is an access list called *103*.

```
Switch(config)# access-list 103 permit 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
```

This example shows how to configure a class map called *dscp_class* whose match criterion is to match IP DSCP 9. A second class map, called *vlan_class*, matches traffic on VLANs 10, 20 to 30, and 40 to class map *dscp_class*:

```
Switch(config)# class-map match-any dscp_class
Switch(config-cmap)# match ip dscp 9
Switch(config-cmap)# exit
Switch(config)# class-map match-all vlan_class
Switch(config-cmap)# match vlan 10 20-30 40
Switch(config-cmap)# match class-map dscp_class
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
match (class-map configuration)	Defines the match criteria to classify traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show class-map	Displays QoS class maps.

clear ip 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

Release	Modification
12.2(25)SEA	This command was introduced.

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
arp access-list	Defines an ARP access control list (ACL).
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show ip arp inspection log	Displays the configuration and contents of the dynamic ARP inspection log buffer.

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*]

Syntax Description

vlan *vlan-range*	(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.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Examples

This example shows how to clear the statistics for VLAN 1:

```
Switch# clear ip arp inspection statistics vlan 1
```

You can verify that the statistics were deleted by entering the **show ip arp inspection statistics vlan 1** privileged EXEC command.

Related Commands

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

clear l2protocol-tunnel counters

Use the **clear l2protocol-tunnel counters** privileged EXEC command to clear the protocol counters in protocol tunnel ports.

clear l2protocol-tunnel counters [*interface-id*]

Syntax Description

interface-id	(Optional) Specify interface (physical interface or port channel) on which to clear protocol counters.

Defaults

This command has no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

Use this command to clear protocol tunnel counters on the switch or on the specified interface.

Examples

This example shows how to clear Layer 2 protocol tunnel counters on an interface:

```
Switch# clear l2protocol-tunnel counters gigabitethernet0/3
```

Related Commands

Command	Description
l2protocol-tunnel	Enable tunneling of Layer 2 protocols on an access or IEEE 802.1Q tunnel port.
show l2protocol-tunnel	Displays information about ports configured for Layer 2 protocol tunneling.

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**]}

Syntax Description

channel-group-number	Channel group number. The range is 1 to 64.
counters	Clear traffic counters.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Examples

This example shows how to clear channel-group information for a specific group:

```
Switch# clear lacp 4
```

This example shows how to clear channel-group traffic counters:

```
Switch# clear lacp counters
```

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

Related Commands

Command	Description
show lacp	Displays LACP channel-group information.

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**}

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **clear mac address-table** command replaces the **clear mac- address-table** command (with the hyphen).

Syntax Description

dynamic	Delete all dynamic MAC addresses.
dynamic address *mac-addr*	(Optional) Delete the specified dynamic MAC address.
dynamic interface *interface-id*	(Optional) Delete all dynamic MAC addresses on the specified physical port or port channel.
dynamic vlan *vlan-id*	(Optional) Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4096.
notification	Clear the notifications in the history table and reset the counters.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	The **notification** keyword was added.
12.1(11)EA1	The **clear mac-address-table** command was replaced by the **clear mac address-table** command.

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

Related Commands

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

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**}

Syntax Description

channel-group-number	Channel group number. The range is 1 to 64.
counters	Clear traffic filters.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Examples

This example shows how to clear channel-group information for a specific group:

```
Switch# clear pagp 10
```

This example shows how to clear channel-group traffic filters:

```
Switch# clear pagp counters
```

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

Related Commands

Command	Description
show pagp	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

all	Delete all secure MAC addresses.
configured	Delete configured secure MAC addresses.
dynamic	Delete secure MAC addresses auto-learned by hardware.
sticky	Delete secure MAC addresses, either auto-learned or configured.
address *mac-addr*	(Optional) Delete the specified dynamic secure MAC address.
interface *interface-id*	(Optional) Delete all the dynamic secure MAC addresses on the specified physical port or VLAN.
vlan	(Optional) Enter one of these options after you enter the **vlan** keyword: • *vlan-id*—On a trunk port, specify the VLAN ID of the VLAN on which this address should be cleared. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)EA1	This command was introduced.
12.1(14)EA1	The **all**, **configured**, and **vlan** keywords were added.
12.2(25)SEB	The **access** and **voice** keywords were added.

Usage Guidelines

If you enter the **clear port-security all** privileged EXEC command, the switch removes all secure MAC addresses from the MAC address table.

If you enter the **clear port-security configured address** *mac-addr* **vlan** *vlan-id* command, the switch removes the specified secure MAC address from the specified VLAN.

If you enter the **clear port-security configured address** *mac-address* command, the switch removes the specified secure MAC address from the MAC address table.

If you enter the **clear port-security dynamic interface** *interface-id* command, the switch removes all dynamic secure MAC addresses on an interface from the MAC address table.

If you enter the **clear port-security sticky** command, the switch removes all sticky secure MAC addresses from the MAC address table.

Examples

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

```
Switch# clear port-security all
```

This example shows how to remove a configured secure address from the MAC address table:

```
Switch# clear port-security configured address 0008.0070.0007
```

This example shows how to remove all the dynamic secure addresses learned on an interface:

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

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

```
Switch# clear port-security sticky
```

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

Related Commands

Command	Description
show port-security	Displays the port security settings for an interface or for the switch.
switchport port-security	Enables port security on an interface.

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*]

Syntax Description

interface *interface-id*	(Optional) Clear all spanning-tree counters on the specified interface. If *interface-id* is not specified, spanning-tree counters are cleared for all interfaces.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(13)EA1	This command was introduced.

Examples

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

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

Related Commands

Command	Description
show spanning-tree	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*]

Syntax Description

interface *interface-id*	(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 64.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

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 an RST BPDU (version 2).

However, the switch does not automatically revert to the rapid-PVST+ or MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

Examples

This example shows how to restart the protocol migration process on an interface:

```
Switch# clear spanning-tree detected-protocols interface fastethernet0/1
```

clear vmps statistics

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

clear vmps statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Examples

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

```
Switch# clear vmps statistics
```

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

Related Commands

Command	Description
show vmps	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

Release	Modification
12.1(4)EA1	This command was introduced.

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
show vtp	Displays general information about the VTP management domain, status, and counters.

cluster commander-address

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

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

no cluster commander-address

Syntax Description

mac-address	MAC address of the cluster command switch.
member *number*	(Optional) Number of a configured member switch. The range is from 0 to 15.
name *name*	(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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

A cluster member can have only one command switch.

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

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

When a standby command switch becomes active (becomes the 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-config

<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
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

cluster discovery hop-count

Use the **cluster discovery hop-count** global configuration command on the 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

Syntax Description

number	Number of hops from the cluster edge that the command switch limits the discovery of candidates. The range is 1 to 7.

Defaults

The hop count is set to 3.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Enter this command only on the command switch. This command does not operate on member switches.

If the hop count is set to 1, it disables extended discovery. The 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 member switch and the first discovered candidate switch.

Examples

This example shows how to set hop count limit to 4. This command is executed on the command switch.

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

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

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	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 this command to remove all members and to make the command switch a candidate switch.

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

no cluster enable

Syntax Description

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

Defaults

The switch is not a command switch.

No cluster name is defined.

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This command runs 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 command switch. If the switch is already configured as the 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 command switch, name the cluster, and set the 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 command switch.

Related Commands

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

cluster holdtime

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

cluster holdtime *holdtime-in-secs*

no cluster holdtime

Syntax Description

holdtime-in-secs	Duration in seconds before a switch (either a command or 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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Use this command with the **cluster timer** global configuration command only on the command switch. The 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 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
show cluster	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 command switch to add candidates to a cluster. Use the **no** form of this 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

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

Defaults

A newly enabled command switch has no associated cluster members.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Enter this command only on the 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 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 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 command-switch password.

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

If you do not specify a VLAN ID, the 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 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
```

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 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 command switch.

Related Commands

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

cluster outside-interface

Use the **cluster outside-interface** global configuration command 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

Syntax Description

interface-id	Interface to serve as the outside interface. Valid interfaces include physical interfaces, port-channels, or VLANs. The port-channel range is 1 to 64. The VLAN range is 1 to 4094.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Enter this command only on the command switch. If you enter this command on a 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.

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

When you enter the **no cluster run** command on a command switch, the command switch is disabled. Clustering is disabled, and the switch is incapable of becoming a candidate switch.

When you enter the **no cluster run** command on a member switch, it is removed from the cluster. Clustering is disabled, and the switch is incapable of becoming 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 command switch:

```
Switch(config)# no cluster run
```

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

Related Commands

Command	Description
show cluster	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 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 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

Syntax Description

HSRP-group-name	Name of the HSRP group that is bound to the cluster. The group name is limited to 32 characters.
routing-redundancy	(Optional) Enable the same HSRP standby group to be used for command-switch redundancy and routing redundancy.

Defaults

The cluster is not bound to any HSRP group.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You must enter this command only on the command switch. If you enter it on a member switch, an error message appears.

The command switch propagates the cluster-HSRP binding information to all cluster-HSRP capable members. Each 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 for 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 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 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
```

This example shows the error message when this command is executed on a 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
standby ip	Enables HSRP on the interface. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show standby	Displays standby group information. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.

cluster timer

Use the **cluster timer** global configuration command on the command switch to set the interval in seconds between heartbeat messages. Use the **no** form of this command to return to the default setting.

cluster timer *interval-in-secs*

no cluster timer

Syntax Description

interval-in-secs	Interval in seconds between heartbeat messages. The range is 1 to 300 seconds.

Defaults

The interval is 8 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Use this command with the **cluster holdtime** global configuration command only on the command switch. The 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 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
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.

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*

Syntax Description

macro-name	Name of the interface-range macro; up to 32 characters.
interface-range	Interface range; for valid values for interface ranges, see "Usage Guidelines."

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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 -5** is a valid range; **gigabitethernet 0/1-5** is not a valid range.

Valid values for *type* and *interface*:

- **vlan** *vlan-id*, where *vlan-id* is from 1 to 4094; do not enter leading zeros
- **port-channel** *port-channel-number*, where *port-channel-number* is 1 to 64
- **fastethernet** *interface-id*
- **gigabitethernet** *interface-id*

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*.

For physical interfaces, the *interface-id* is defined as slot/number (where slot is always 0 for the switch), and the range can be entered as one of the following:

- *type* **0**/*number* - *number* (for example, **gigabitethernet0/1 -2**)
- type **0**/*number* - **0**/*number* (for example, **gigabitethernet 0/1 - 0/2**)

You can also enter multiple ranges.

When you define a range, you must enter a space before and after the hyphen (-), for example, **gigabitethernet0/1 - 2**

When you define multiple ranges, you must enter a space before and after the comma (,), for example, **fastethernet0/3 - 7 , gigabitethernet0/1 - 2**

Examples

This example shows how to create a multiple-interface macro:

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 -2, gigabitethernet0/5
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.
show running-config	Displays the current operating configuration, including defined macros. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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

/force	(Optional) Suppress the prompt that confirms the deletion.
/recursive	(Optional) Delete the named directory and all subdirectories and the files contained in it.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	The path (directory) and filename to delete.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If you use the **/force** keyword, you are prompted 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
archive download-sw	Downloads a new image to the switch and overwrites or keeps the existing image.

deny

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**]

Note Though visible in the command-line help strings, **appletalk** is not supported as a matching condition, nor is matching on any SNAP-encapsulated packet with a non-zero Organizational Unique Identifier (OUI).

Syntax Description

any	Keyword to specify to deny any source or destination MAC address.
host *src MAC-addr* | *src-MAC-addr mask*	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.
host *dst-MAC-addr* | *dst-MAC-addr mask*	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.
type mask	(Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. The *type* is 0 to 65535, typically specified in hexadecimal. The *mask* is a mask of *don't care* bits applied to the Ethertype before testing for a match.
aarp	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Select EtherType DEC-Amber.
cos *cos*	(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 **cos** option is configured.
dec-spanning	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Select EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Select EtherType DEC-Diagnostic.
dsm	(Optional) Select EtherType DEC-DSM.
etype-6000	(Optional) Select EtherType 0x6000.
etype-8042	(Optional) Select EtherType 0x8042**.**

lat	(Optional) Select EtherType DEC-LAT.
lavc-sca	(Optional) Select EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Use the LSAP number (0 to 65535) of a packet with IEEE 802.2 encapsulation to identify the protocol of the packet. *mask* is a mask of *don't care* bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Select EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Select EtherType DEC-MOP Dump.
msdos	(Optional) Select EtherType DEC-MSDOS.
mumps	(Optional) Select EtherType DEC-MUMPS.
netbios	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Select EtherType VINES IP.
xns-idp	(Optional) Select EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.

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 2-3.

Table 2-3 IPX Filtering Criteria

IPX Encapsulation Type		
Cisco IOS Name	**Novel Name**	**Filter Criterion**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet IEEE 802.2	LSAP 0xE0E0
novell-ether	Ethernet IEEE 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

Release	Modification
12.1(4)EA1	This command was introduced.

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.

Note 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
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits non-IP traffic to be forwarded if conditions are matched.
show access-lists	Displays access control lists configured on a switch.

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**]

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

request	(Optional) Define a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets.
ip	Specify the sender IP address.
any	Deny any IP or MAC address.
host *sender-ip*	Deny the specified sender IP address.
sender-ip sender-ip-mask	Deny the specified range of sender IP addresses.
mac	Deny the sender MAC address.
host *sender-mac*	Deny a specific sender MAC address.
sender-mac sender-mac-mask	Deny the specified range of sender MAC addresses.
response ip	Define the IP address values for the ARP responses.
host *target-ip*	Deny the specified target IP address.
target-ip target-ip-mask	Deny the specified range of target IP addresses.
mac	Deny the MAC address values for the ARP responses.
host *target-mac*	Deny the specified target MAC address.
target-mac target-mac-mask	Deny the specified range of target MAC addresses.
log	(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

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

You can add deny clauses to drop ARP packets based on matching criteria.

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

Command	Description
arp access-list	Defines an ARP access control list (ACL).
ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
permit (ARP access-list configuration)	Permits an ARP packet based on matches against the DHCP bindings.
show arp access-list	Displays detailed information about ARP access lists.

dot1x

Use the **dot1x** global configuration command to enable IEEE 802.1x authentication globally. Use the **no** form of this command to return to the default setting.

dot1x {**critical** {**eapol** | **recovery delay** *milliseconds*} | **system-auth-control**}

no dot1x {**credentials** | **critical** {**eapol** | **recovery delay**} | **system-auth-control**}

Note Though visible in the command-line help strings, the **credentials** *name* keywords are not supported.

Syntax Description

critical {**eapol** | **recovery delay** *milliseconds*}	Configure the inaccessible authentication bypass parameters. For more information, see the **dot1x critical (global configuration)** command.
system-auth-control	Enable IEEE 802.1x authentication globally on the switch.

Defaults

IEEE 802.1x authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.2(25)SE	The **guest-vlan supplicant** keywords were added.
12.2(25)SEE	The **critical** {**eapol** | **recovery delay** *milliseconds*} keywords were added. The **guest-vlan supplicant keyword** was removed.

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 queried 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 and your switch is running Cisco IOS Release 12.1(14)EA1, make sure that the device is running ACS Version 3.2.1 or later.

Examples

This example shows how to enable IEEE 802.1x authentication globally on a switch:

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

You can verify your settings by entering the **show dot1x** privileged EXEC command.

Related Commands

Command	Description
dot1x guest-vlan	Enables and specifies an active VLAN as an IEEE 802.1x guest VLAN.
dot1x port-control	Enables manual control of the authorization state of the port.
show dot1x	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x auth-fail max-attempts

Use the **dot1x auth-fail max-attempts** interface configuration command to configure the maximum number of authentication attempts allowed 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

Syntax Description

max-attempts	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.

Defaults

The default is 3 attempts.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

If you reconfigure the maximum number of authentication failures allowed by the VLAN, the change takes effect after the re-authentication timer expires.

Examples

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 Gigabit Ethernet interface 3:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
dot1x auth-fail vlan [*vlan id*]	Enables the optional restricted VLAN feature.

Command	Description
dot1x max-reauth-req [*count*]	Sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

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 *vlan-id*

Syntax Description

vlan-id	Specify a VLAN in the range of 1 to 4094.

Defaults

No restricted VLAN is configured.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can configure a restricted VLAN on ports configured as follows:

- single-host (default) mode only
- auto mode for authorization

You should enable re-authentication. The ports in restricted VLANs do not receive re-authentication requests if re-authentication 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 the host is connected through a hub, the port might never receive a link down event and might not detect the new host until the next re-authentication attempt occurs. Therefore, re-authentication should be enabled.

If the user fails authentication, the port is moved to a restricted VLAN, and an EAP success message is sent to the user. Because the user is not notified of the authentication failure, there might be confusion as to why there is restricted access to the network. An EAP success message is sent for these reasons:

- If the EAP success message is not sent, the user 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 user 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 user passes the correct username and password combination, the port remains in the restricted VLAN.

Internal VLANs that are used for Layer 3 ports cannot be configured as a restricted VLAN.

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 is restarted. If the user fails the authentication process again, the authenticator waits in the held state. After the user 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 to a different VLAN, any ports in the restricted VLAN are also moved and the ports stay in their current 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 is restarted. 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. As soon as the restricted VLAN becomes active, the port is placed in the restricted VLAN.

The restricted VLAN is supported only in single-host mode (the default port mode).

When a port is placed in a restricted VLAN, the user's MAC address is added to the MAC address table. If a new MAC address appears on the port, it is treated as a security violation.

Examples

This example shows how to configure a restricted VLAN on Gigabit Ethernet interface 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x auth-fail vlan 40
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
dot1x auth-fail max-attempts [*max-attempts*]	Configures the number of authentication attempts allowed before assigning a user to the restricted VLAN.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

dot1x control-direction

Use the **dot1x control-direction** interface configuration command to configure the IEEE 802.1x authentication with the wake-on-LAN (WoL) feature 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 {**in** | **both**}

no dot1x control-direction {**in** | **both**}

Syntax Description

in	Enable bidirectional control on port. The port cannot receive packets from or send packets to the host.
both	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.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEC	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.

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
```

These examples show 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:

```
Supplicant 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
show dot1x all [**interface** *interface-id*]	Displays control-direction port setting status for the 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**}

Syntax Description

eapol	Specify that the switch sends an EAPOL-Success message when the switch puts the critical port in the critical-authentication state.
recovery delay *milliseconds*	Set the recovery delay period in milliseconds. The range is from 1 to 10000 milliseconds.

Defaults

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).

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

Usage Guidelines

Use the **eapol** 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 **recovery delay** *milliseconds* 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 100 milliseconds. A port can be re-initialized every second.

To enable inaccessible authentication bypass on a port, use the **dot1x critical** interface configuration command. To configure the access VLAN to which the switch assigns a critical port, use the **dot1x critical vlan** *vlan-id* interface configuration command.

Examples

This example shows how to set 200 as the recovery delay period on the switch:

```
Switch# dot1x critical recovery delay 200
```

You can verify your configuration by entering the **show dot1x** privileged EXEC command.

Related Commands

Command	Description
dot1x critical (interface configuration)	Enables the inaccessible authentication bypass feature, and configures the access VLAN for the feature.
show dot1x	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**]

Syntax Description

recovery action reinitialize	Enable the inaccessible-authentication-bypass recovery feature, and specify that the recovery action is to authenticate the port when an authentication server is available.
vlan *vlan-id*	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

Release	Modification
12.2(25)SEE	This command was introduced.

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 criticalport 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.

Examples

This example shows how to enable the inaccessible authentication bypass feature on port 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/1
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
dot1x critical (global configuration)	Configures the parameters for the inaccessible authentication bypass feature on the switch.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

dot1x default

Use the **dot1x default** interface configuration command to reset the configurable 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-interface 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

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	This command was changed to the interface configuration mode.

Examples

This example shows how to reset the configurable IEEE 802.1x parameters on an interface:

```
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
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

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

Syntax Description

vlan-id	Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094.

Defaults

No guest VLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.2(25)SE	The default behavior of this command changed.

Usage Guidelines

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 currently running IEEE 802.1x authentication. These users might be upgrading their system 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.

With Cisco IOS Release 12.2(25)SE and later, 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.

Before Cisco IOS Release 12.2(25)SE, the switch did not maintain the EAPOL packet history and allowed clients that failed authentication access to the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. In Cisco IOS Release 12.2(25)SE, you can use the **dot1x guest-vlan supplicant** global configuration command to enable this optional behavior.

However, in Cisco IOS Release 12.2(25)SEE, the **dot1x guest-vlan supplicant** global configuration command is no longer supported. You can use a restricted VLAN to allow clients that failed authentication access to the network by entering the **dot1x auth-fail vlan** *vlan-id* interface configuration command.

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-specified 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 internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

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 also 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* in Cisco IOS Release 12.2(25)SEE and later. When MAC authentication bypass 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 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)# interface FastEthernet0/1
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

Command	Description
dot1x	Enables the optional guest VLAN supplicant feature.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

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 that has the **dot1x port-control** interface configuration command set to **auto**. Use the **no** form of this command to return to the default setting.

dot1x host-mode {**multi-host** | **single-host**}

no dot1x host-mode [**multi-host** | **single-host**]

Syntax Description

multi-host	Enable multiple-hosts mode on the switch.
single-host	Enable single-host mode on the switch.

Defaults

The default is single-host mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced. It replaces the **dot1x multiple-hosts** interface configuration command.

Usage Guidelines

You can 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 must 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.

Before entering this command, make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.

Examples

This example shows how to enable IEEE 802.1x authentication globally, enable IEEE 802.1x authentication on an interface, and enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return an IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the interface.

dot1x initialize interface *interface-id*

Syntax Description

This command has no arguments or keywords.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)EA1	This command was introduced.

Usage Guidelines

Use this command to manually return a device connected to a switch interface to an unauthorized state before initiating a new authentication session on the interface.

Examples

This example shows how to manually return a device connected to an interface to an unauthorized state:

```
Switch# dot1x initialize interface fastethernet0/1
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

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**]

no dot1x mac-auth-bypass

Syntax Description

eap	(Optional) Configure the switch to use Extensible Authentication Protocol (EAP) for authentication.

Defaults

MAC authentication bypass is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

Usage Guidelines

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.lx 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
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

dot1x max-reauth-req

Use the **dot1x max-reauth-req** interface configuration command on the switch stack or on a standalone switch 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	Number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 0 to 10.

Defaults

The default is 2 times.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SE	This command was introduced.
12.2(25)SEC	The *count* range changed.

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
dot1x max-req	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.
dot1x timeout tx-period	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.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

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

Syntax Description

count	Number of times that the switch sends an EAP frame from the authentication server before restarting the authentication process. The range is 1 to 10.

Defaults

The default is 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	This command was changed to the interface configuration mode.

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 5 as the number of times that the switch sends an EAP frame from the authentication server 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.

Related Commands

Command	Description
dot1x timeout	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.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

dot1x multiple-hosts

This is an obsolete command.

In past releases, the **dot1x multiple-hosts** interface configuration command was used to allow multiple hosts (clients) on an IEEE 802.1x-authorized port.

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	The **dot1x multiple-hosts** interface configuration command was replaced by the **dot1x host-mode** interface configuration command.

Related Commands

Command	Description
dot1x host-mode	Set the IEEE 802.1x host mode on an interface.
show dot1x	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified interface.

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

Syntax Description

This command has no arguments or keywords.

Defaults

The port is not an IEEE 802.1x PAE authenticator, and IEEE 802.1x authentication is disabled on the port.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

Usage Guidelines

Use the **no dot1x pae** interface configuration command to disable IEEE 802.1x authentication on the port.

When you configure IEEE 802.1x authentication on a port, such as entering the **dot1x port-control** interface configuration command, the switch automatically configures the port as an EEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is enabled.

Examples

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.

Related Commands

Command	Description
show dot1x	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.
show eap	Displays EAP registration and session information for the switch or for the specified port.

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 interface and cause the port to transition 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 interface and cause the port to transition to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client.
force-unauthorized	Deny all access through this interface by forcing the port to transition to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

Defaults

The default is force-authorized.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

You must enable IEEE 802.1x authentication globally on the switch by using the **dot1x system-auth-control** global configuration command before enabling IEEE 802.1x authentication on a specific interface.

The IEEE 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports.

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 authentication 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.
- 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, 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.

Note In software releases earlier than Cisco IOS Release 12.2(25)SE, if IEEE 802.1x authentication is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

- Switched Port Analyzer (SPAN) destination port—You can enable IEEE 802.1x authentication on a port that is a SPAN destination port; however, IEEE 802.1x authentication is disabled until the port is removed as a SPAN destination. You can enable IEEE 802.1x authentication on a SPAN source port.

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

Examples

This example shows how to enable IEEE 802.1x authentication on an interface:

```
Switch(config)# interface fastethernet0/1
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
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

dot1x re-authenticate

Use the **dot1x re-authenticate** privileged EXEC command to manually initiate a re-authentication of the IEEE 802.1x-enabled port.

dot1x re-authenticate {**interface** *interface-id*}

Syntax Description

interface *interface-id*	Slot and port number of the interface to re-authenticate.

Defaults

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

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.

Examples

This example shows how to manually re-authenticate the device connected to an interface:

```
Switch# dot1x re-authenticate interface fastethernet0/1
```

Related Commands

Command	Description
show dot1x	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authentication

This is an obsolete command.

In past releases, the **dot1x re-authentication** global configuration command was used to set the amount of time between periodic re-authentication attempts.

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	The **dot1x reauthentication** interface configuration command replaced the **dot1x re-authentication** global configuration command.

Related Commands

Command	Description
dot1x reauthentication	Sets the number of seconds between re-authentication attempts.
show dot1x	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified interface.

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

Release	Modification
12.1(14)EA1	This command was introduced. It replaces the **dot1x re-authentication** global configuration command (with the hyphen).

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
dot1x timeout	Sets the number of seconds between re-authentication attempts.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

dot1x timeout

Use the **dot1x timeout** interface configuration command to set the 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

quiet-period *seconds*	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.
ratelimit-period *seconds*	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.
reauth-period *seconds*	Set the number of seconds between re-authentication attempts. The keywords have these meanings: • *seconds*—Sets the number of seconds from 1 to 65535; the default is 3600 seconds. • **server**—Sets the number of seconds as the value of the Session-Timeout RADIUS attribute (Attribute[27]).
server-timeout *seconds*	Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. The range is 30 to 65535.
supp-timeout *seconds*	Number of seconds that the switch waits for the retransmission of packets by the switch to the client. The range is 30 to 65535.
tx-period *seconds*	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 5 to 65535.

Defaults

These are the defaults:

quiet-period is 60 seconds.

rate-limit is 0 seconds.

reauth-period is 3600 seconds.

server-timeout is 30 seconds.

supp-timeout is 30 seconds.

tx-period is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	The **supp-timeout** and **server-timeout** keywords were added, and the command was changed to the interface configuration mode.
12.1(22)EA5	The **reauth-period server** keywords were added
12.2(25)SE	The ranges for the **server-timeout**, **supp-timeout**, and **tx-period** keywords were changed.
12.2(25)SEC	The range for the **tx-period** keyword was changed, and the **reauth-period server** keywords were added.
12.2(25)SEE	The **ratelimit-period** keyword was introduced.

Usage Guidelines

You should change the default values 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 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 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 45 seconds as the switch-to-authentication server retransmission time:

```
Switch(config)# dot1x timeout server-timeout 45
```

This example shows how to return to the default re-authorization period:

```
Switch(config-if)# no dot1x timeout reauth-period
```

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** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.
dot1x reauthentication	Enables periodic re-authentication of the client.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified interface.

duplex

Use the duplex interface configuration command to specify the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports. Use the **no** form of this command to return to the default setting.

duplex {**auto** | **full** | **half**}

no duplex

Note This command is not available on Gigabit Interface Converter (GBIC) ports. The default duplex on GBIC ports is autonegotiation.

Syntax Description

auto	Port automatically detects whether it should run in full- or half-duplex mode.
full	Port is in full-duplex mode.
half	Port is in half-duplex mode.

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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.

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.

You cannot configure duplex mode on GBIC interfaces.

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.

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.

Beginning with Cisco IOS Release 12.1(22)EA1, you can configure the duplex setting when the speed is set to **auto**.

If both the speed and duplex are set to specific values, autonegotiation is disabled.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Note For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

Examples

This example shows how to configure an interface for full duplex operation:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# duplex full
```

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

Related Commands

Command	Description
show interfaces	Displays the interface settings on the switch.
speed	Sets the speed on a 10/100/1000 Mbps interface.

errdisable detect cause

Use the **errdisable detect cause** global configuration command to enable error disable detection for a specific cause or all causes. Use the **no** form of this command to disable the error disable detection feature.

errdisable detect cause {**all** | **arp-inspection** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap**}

no errdisable detect cause {**all** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap**}

Syntax Description

all	Enable error detection for all error-disable states.
arp-inspection	Enable error detection for dynamic Address Resolution Protocol (ARP) inspection.
dhcp-rate-limit	Enable error detection for the DHCP rate limit cause.
dtp-flap	Enable error detection for the Dynamic Trunking Protocol (DTP) flap error-disable cause.
gbic-invalid	Enable error detection for an invalid GBIC error-disable cause.
l2ptguard	Enable error detection for a Layer 2 protocol-tunnel error-disable cause.
link-flap	Enable error detection for the link flap error-disable cause.
loopback	Enable error detection for detected loopbacks.
pagp-flap	Enable error detection for the Port Aggregation Protocol (PAgP) flap-error disable cause.

Note Though visible in the command-line help strings, the **arp-inspection** keyword is not supported.

Defaults

Detection is enabled for all causes.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	The **bpduguard**, **rootguard,** and **udld** keywords were removed.
12.1(9)EA1	The **l2ptguard** and **gbic-invalid** keywords were added.
12.1(13)EA1	The **loopback** keyword was added.
12.1(19)EA1	The **dhcp-rate-limit** and **loopback** keywords were added.
12.2(25)SEA	The **arp-inspection** keyword was added.

Usage Guidelines

A cause (**dhcp-rate-limit**, **dtp-flap**, and so forth) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command for the cause, the interface 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 recover an interface from the error-disabled state.

Examples

This example shows how to enable error disable detection for the link-flap error-disable cause:

```
Switch(config)# errdisable detect cause link-flap
```

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

Related Commands

Command	Description
show errdisable detect	Displays error-disabled detection information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in 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** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **udld** | **vmps**}} | {**interval** *interval*}

no errdisable recovery {**cause** {**all** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **udld** | **vmps**}} | {**interval** *interval*}

Syntax Description

cause	Enable error disable to recover from a specific cause.
all	Enable the timer to recover from all error-disable causes.
arp-inspection	Enable the timer to recover from the Address Resolution Protocol (ARP) inspection error-disable state.
bpduguard	Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disable state.
channel-misconfig	Enable the timer to recover from the EtherChannel misconfiguration error-disable state.
dhcp-rate-limit	Enable the timer to recover from the DHCP error-disable state.
dtp-flap	Enable the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disable state.
gbic-invalid	Enable the timer to recover from an invalid GBIC error-disable state.
l2ptguard	Enable the timer to recover from a Layer 2 protocol tunnel error-disable state.
link-flap	Enable the timer to recover from the link-flap error-disable state.
loopback	Enable the timer to recover from a loopback error-disable state.
pagp-flap	Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disable state.
psecure-violation	Enable the timer to recover from a port security violation disable state.
security-violation	Enable the timer to recover from an IEEE 802.1x violation disable state
udld	Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disable state.
vmps	Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disable state.
interval *interval*	Specify the time to recover from the specified error-disable state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds. **Note** 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.

Note Though visible in the command-line help strings, the **arp-inspection**, **storm-control**, and **unicast-flood** keywords are not supported.

Defaults

Recovery is disabled for all causes.

The default recovery interval is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	The **rootguard** keyword was deleted.
12.1(9)EA1	The **gbic-invalid**, **l2ptguard**, and **psecure-violation** keywords were added.
12.1(13)EA1	The **channel-misconfig** keyword was added.
12.1(19)EA1	The **dhcp-rate-limit**, **loopback**, **security-violation**, and **vmps** keywords were added.
12.2(25)SEA	The **arp-inspection** keyword was added.

Usage Guidelines

A cause (**bpduguard**, **dhcp-rate-limit**, and so forth) is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable the recovery for the cause, the interface stays in error-disabled state until you enter a **shutdown** and **no shutdown** interface configuration command. If you enable the recovery for a cause, the interface 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** then **no shutdown** commands to manually recover an interface from the error-disabled state.

Examples

This example shows how to enable the recovery timer for the BPDU guard error-disable 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
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in error-disabled state.

flowcontrol

Use the **flowcontrol** interface configuration command to set the receive or send flow-control value for an interface. When flow control **send** is 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 the remote 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** and **send off** keywords to disable flow control.

flowcontrol {**receive** | **send**} {**desired** | **off** | **on**}

Note On the Catalyst 3550 switch, Gigabit Ethernet ports can receive and send pause frames; Fast Ethernet ports can receive only pause frames. Therefore, for 10/100 ports, the **send** keyword is not available.

Syntax Description

receive	Set whether the interface can receive flow-control packets from a remote device.
send	Set whether the interface can send flow-control packets to a remote device. This keyword is not available for 10/100 Mbps interfaces.
desired	When used with **receive**, allows 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. When used with **send**, the interface sends flow-control packets to a remote device if the remote device supports it.
off	When used with **receive**, turns off an attached device's ability to send flow-control packets to an interface. When used with **send**, turns off the local port's ability to send flow-control packets to a remote device.
on	When used with **receive**, allows 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. When used with **send**, the interface sends flow-control packets to a remote device if the remote device supports it.

Defaults

The defaults for Gigabit Ethernet interfaces are **flowcontrol receive off** and **flowcontrol send desired**. The defaults for Fast Ethernet interfaces are **flowcontrol receive off** and **flowcontrol send off**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You must not configure both IEEE 802.3z flow control and quality of service (QoS) on a switch. Before configuring flow control on an interface, use the **no mls qos** global configuration command to disable QoS on the switch.

Note that when used with **receive**, the **on** and **desired** keywords have the same result.

Note On the switch, 10/100/1000 Mbps and GBIC ports can receive and send pause frames; 10/100 Mbps ports can receive only pause frames. Therefore, for 10/100 ports, the conditions described in the next paragraphs are always **send off**.

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** and **send on**: Flow control operates in both directions; pause frames can be sent by both the local device and the remote device to show link congestion.
- **receive on** and **send desired**: The port can receive pause frames and is able to send pause frames if the attached device supports it.
- **receive on** and **send off**: The port cannot send out pause frames, but can operate with an attached device that is required to or is able to send pause frames; the port is able to receive pause frames.
- **receive off** and **send on**: The port sends pause frames if the remote device supports it, but cannot receive pause frames from the remote device.
- **receive off** and **send desired**: The port cannot receive pause frames, but can send pause frames if the attached device supports it.
- **receive off** and **send 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.

Table 2-4 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. Because 10/100 Mbps ports cannot send pause frames, only the last two rows (**send off**) apply to these ports.

Table 2-4 Flow Control Settings and Local and Remote Port Flow Control Resolution

Flow Control Settings		Flow Control Resolution	
Local Device	**Remote Device**	**Local Device**	**Remote Device**
send on/receive on	**send on/receive on**	Sends and receives	Sends and receives
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Sends and receives	Sends and receives
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Sends and receives	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send on/receive off	**send on/receive on**	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Sends only	Receives only
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Sends only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive

Table 2-4 Flow Control Settings and Local and Remote Port Flow Control Resolution (continued)

Flow Control Settings		Flow Control Resolution	
Local Device	**Remote Device**	**Local Device**	**Remote Device**
send desired/receive on	**send on/receive on**	Sends and receives	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Sends and receives	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Sends and receives	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send desired/receive off	**send on/receive on**	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Sends only	Receives only
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Sends only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive on	**send on/receive on**	Receives only	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Receives only	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Receives only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive off	**send on/receive on**	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Does not send or receive	Does not send or receive
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Does not send or receive	Does not send or receive
	send off/receive off	Does not send or receive	Does not send or receive

Examples

This example shows how to configure the local port to not support any level of flow control by the remote port:

```
Switch(config-if)# flowcontrol receive off
Switch(config-if)# flowcontrol send off
```

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

Related Commands

Command	Description
show interfaces flowcontrol	Displays interface input and output flow control settings and status.
show flowcontrol	Displays flow control settings and status for specified interfaces or all interfaces on the switch.

interface port-channel

Use the **interface port-channel** global configuration command to access or create the port-channel logical interface for Layer 3 routed interfaces. 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 64.

Defaults

No port-channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you must configure the **channel-group** interface configuration command, which automatically creates the port-channel logical interface. You cannot put Layer 2 interfaces into a manually created port-channel interface.

You create Layer 3 port channels by using the **interface port-channel** command. You must manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.

Caution When using a port-channel interface as a routed interface, do not assign Layer 3 addresses on the physical interfaces that are assigned to the channel group.

Caution Do not assign bridge groups on the physical interfaces in a channel group used as a Layer 3 port-channel interface because it creates loops. You must also disable spanning tree.

Follow these guidelines when you use the **interface port-channel** command:

- If you configure Inter-Switch Link (ISL), you must assign the IP address to the switch virtual interface (SVI).
- If you want to use the CDP, you must configure it only on the physical interface and not on the port-channel interface.

- If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- Before enabling IEEE 802.1x authentication on a port, you must first remove it from the EtherChannel. If you try to enable IEEE 802.1x authentication on an EtherChannel or on an active port in an EtherChannel, an error message appears, and IEEE 802.1x authentication is not enabled.

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

Command	Description
channel-group	Assigns an Ethernet interface to an EtherChannel group.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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*}

Syntax Description

port-range	Port range. For a list of valid values for *port-range*, see the "Usage Guidelines" section.
macro *name*	Specify the name of a macro.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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

You can define up to five interface ranges with a single command, with each range separated by a comma.

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.

Valid values for *port-range* type and interface:

- **vlan** *vlan-id*, where *vlan-id* is 1 to 4094; do not enter leading zeros
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 64
- **fastethernet** *interface-id*
- **gigabitethernet** *interface-id*

For physical interfaces, the *interface-id* is defined as a slot/number (where slot is always 0 for the switch), and you can enter the range in one of these ways:

- *type* **0**/*number* - *number* (for example, **gigabitethernet0/1 -2**)
- type **0**/*number* - **0**/*number* (for example, **gigabitethernet0/1 - 0/2**)

When you define a range, you must enter a space between the first entry and the hyphen (-):

```
interface range gigabitethernet0/1 -2, gigabitethernet0/4 -5
```

When you define multiple ranges, you must enter a space before and after the comma (,):

```
interface range fastethernet0/3 - 7, gigabitethernet0/1 - 2
```

You cannot specify both a macro and an interface range in the same command.

A single interface can also be specified in *port-range* (this would make the command similar to the **interface** *interface-id* global configuration command).

Note 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:

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

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)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

Related Commands

Command	Description
define interface-range	Creates an interface range macro.
show running-config	Displays the configuration information currently running on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

interface vlan

Use the **interface vlan** global configuration command to create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode. Use the **no** form of this command to delete an SVI.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number from 1 to 4094; do not enter leading zeros.

Defaults

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular *vlan*. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an ISL or IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the deleted interface is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration will be gone.

The number of routed ports and SVIs that you can configure is not limited by software; however, the interrelationship between this number and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables. For the Catalyst 3550 Gigabit Ethernet switches, the tables are based on 16 routed interfaces (SVIs and routed ports. For switches with mainly Fast Ethernet ports, the tables are based on 8 routed interfaces. For more information, see the **sdm prefer** command.

Examples

This example shows how to create a new SVI with VLAN ID 23 and 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

Command	Description
show interfaces vlan *vlan-id*	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

access-list-number	The number of the IP access control list (ACL). The range is 1 to 199 and 1300 to 2699.
name	The name of an IP ACL, specified in the **ip access-list** global configuration command.
in	Specify filtering on inbound packets.
out	Specify filtering on outbound packets. This keyword is valid only on Layer 3 interfaces.

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You can apply named or numbered standard or extended 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 used 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 for Layer 2 interfaces (port ACLs):

- You can only apply ACLs in the inbound direction; the **out** keyword is not supported for Layer 2 interfaces.
- You can only apply one IP ACL and one MAC ACL per interface.
- Layer 2 interfaces do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to a Layer 2 interface only filters IP packets. To filter non-IP packets, use the **mac access-group** interface configuration command with MAC extended ACLs.

You can apply IP ACLs to both outbound or inbound Layer 3 interfaces.

A Layer 2 interface can have only one IP ACL applied (in the inbound direction). A Layer 3 interface can have one IP ACL applied in each direction.

You cannot apply an IP ACL to a Layer 3 interface on a switch that has a Layer 2 interface with an applied IP ACL or MAC ACL, and you cannot apply a VLAN map to any of the switch VLANs.

You cannot apply an IP ACL or MAC ACL to a Layer 2 interface on a switch that has an input Layer 3 ACL or a VLAN map applied to it.

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 access list has been applied to a Layer 3 interface, discarding a packet (by default) causes the generation of an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP Host Unreachable messages are not generated for packets discarded on a Layer 2 interface.

For standard outbound access lists, after receiving a packet and sending it to a controlled interface, the switch checks the packet against the access list. If the access list permits the packet, the switch sends the packet. If the access list denies the packet, the switch discards the packet and, by default, generates an ICMP Host Unreachable message.

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 an interface:

```
Switch(config)# interface fastethernet0/1
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

Command	Description
access list	Configures a numbered ACL. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2** > **IP Services Commands**.
ip access-list	Configures a named ACL. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2** > **IP Services Commands**.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2** > **IP Services Commands**.
show ip interface	Displays information about interface status and configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2** > **IP Services Commands**.

ip address

Use the **ip address** interface configuration command to set an IP address for the Layer 2 switch or an IP address for each switch virtual interface (SVI) or routed port on the Layer 3 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

ip-address	IP address.
subnet-mask	Mask for the associated IP subnet.
secondary	(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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch is lost.

Hosts can find subnet masks by sending an 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 sends 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.

When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or DHCP server cannot reassign the address.

A Layer 3 switch can have an IP address assigned to each routed port and SVI. The number of routed ports and SVIs that you can configure is not limited by software; however, the interrelationship between this number and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables. For the Catalyst 3550 Gigabit Ethernet switches, the tables are based on 16 routed interfaces (SVIs and routed ports. For switches with mainly Fast Ethernet ports, the tables are based on 8 routed interfaces. For more information, see the sdm prefer command.

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
```

This example shows how to configure the IP address for a port on the Layer 3 switch:

```
Switch(config)# ip multicast-routing
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

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

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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**]

Syntax Description

arp-acl-name	ARP access control list (ACL) name.
vlan-range	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.
static	(Optional) Specify **static** 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

Release	Modification
12.2(25)SEA	This command was introduced.

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
arp access-list	Defines an ARP ACL.
deny (ARP access-list configuration)	Denies an ARP packet based on matches against the DHCP bindings.
permit (ARP access-list configuration)	Permits an ARP packet based on matches against the DHCP bindings.
show arp access-list	Displays detailed information about ARP access lists.
show ip arp inspection vlan *vlan-range*	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

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 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

Syntax Description

rate *pps*	Specify an upper limit for the number of incoming packets processed per second. The range is 0 to 2048 packets per second (pps).
burst interval *seconds*	(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.
none	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

Release	Modification
12.2(25)SEA	This command was introduced.

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-disable 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 to 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)# interface gigabitethernet 0/1
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
show ip arp inspection interfaces	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.

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**}

Syntax Description

entries *number*	Number of entries to be logged in the buffer. The range is 0 to 1024.
logs *number* **interval** *seconds*	Number of entries needed in the specified interval to generate system messages. For **logs** *number*, 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 **interval** *seconds*, 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

Release	Modification
12.2(25)SEA	This command was introduced.

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 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
arp access-list	Defines an ARP access control list (ACL).
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show ip arp inspection log	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

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

This command has no arguments or keywords.

Defaults

The interface is untrusted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

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)# interface gigabitethernet 0/1
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
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
show ip arp inspection interfaces	Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.
show ip arp inspection log	Displays the configuration and contents of the dynamic ARP inspection log buffer.

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**]}

no ip arp inspection validate [**src-mac**] [**dst-mac**] [**ip**]

Syntax Description

src-mac	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.
dst-mac	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.
ip	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 compared only in ARP responses.

Defaults

No checks are performed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

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.

If you first specify the **src-mac** keyword, you also can specify the **dst-mac** and **ip** keywords. If you first specify the **ip** keyword, no other keywords can be specified.

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 show 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
show ip arp inspection vlan *vlan-range*	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*

Syntax Description

vlan-range	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.

Defaults

ARP inspection is disabled on all VLANs.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

You must specify the VLANs on which to enable dynamic ARP inspection.

Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

Examples

This example shows how to enable dynamic ARP inspection on VLAN 1:

```
Switch(config)# ip arp inspection vlan 1
```

You can verify your setting by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

Related Commands

Command	Description
arp access-list	Defines an ARP access control list (ACL).
show ip arp inspection vlan *vlan-range*	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**}}

no ip arp inspection vlan *vlan-range* **logging** {**acl-match** | **dhcp-bindings**}

Syntax Description

vlan-range	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.
acl-match {**matchlog** | **none**}	Specify that the logging of packets is based on access control list (ACL) matches. The keywords have these meanings: • **matchlog**—Log packets based on the logging configuration specified in the access control entries (ACE). If you specify the **matchlog** keyword in this command and the **log** keyword in the **permit** or **deny** ARP access-list configuration command, Address Resolution Protocol (ARP) packets permitted or denied by the ACL are logged. • **none**—Do not log packets that match ACLs.
dhcp-bindings {**permit** | **all** | **none**}	Specify the logging of packets is based on Dynamic Host Configuration Protocol (DHCP) binding matches. The keywords have these meanings: • **all**—Log all packets that match DHCP bindings. • **none**—Do not log packets that match DHCP bindings. • **permit**—Log DHCP-binding permitted packets.

Defaults

All denied or all dropped packets are logged.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

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 Address Resolution Protocol (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

Command	Description
arp access-list	Defines an ARP ACL.
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
show ip arp inspection log	Displays the configuration and contents of the dynamic ARP inspection log buffer.
show ip arp inspection vlan *vlan-range*	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

ip dhcp snooping

Use the **ip dhcp snooping** global configuration command to enable DHCP snooping globally. 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

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

You must globally enable DHCP snooping for any DHCP snooping configuration to take effect.

DHCP snooping is not active until snooping is enabled on a VLAN by using the **ip dhcp snooping VLAN** *vlan-id* global configuration command.

In Cisco IOS Release 12.1(19)EA1, the implementation for the option-82 subscriber identification changed from the previous release. The new option-82 format uses a different circuit ID and remote ID suboption, **vlan-mod-port**. The previous version uses the **snmp-ifindex** circuit ID and remote ID suboption.

If you have option 82 configured on the switch and you upgrade to Cisco IOS Release 12.1(19)EA1 or later, the option-82 configuration is not affected. However, when you enable DHCP snooping globally on the switch by using the **ip dhcp snooping** global configuration command, the previous option-82 configuration is suspended, and the new option-82 format is applied. When you disable DHCP snooping on the switch, the previous option-82 configuration is re-enabled.

To provide for backward compatibility, you can select the previous option-82 format by using the **ip dhcp snooping information option format snmp-ifindex** global configuration command when you enable DHCP snooping. When DHCP snooping is enabled globally, option-82 information (in the selected format) is inserted only on snooped VLANs.

To use the previous version of option 82 without enabling DHCP snooping, see the software configuration guide for more information.

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** privileged EXEC command.

Related Commands

Command	Description
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	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*

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

mac-address	Specify a MAC address.
vlan *vlan-id*	Specify a VLAN number. The range is from 1 to 4904.
ip-address	Specify an IP address.
interface *interface-id*	Specify an interface on which to add or delete a binding entry.
expiry *seconds*	Specify the interval (in seconds) after which the binding entry is no longer valid. The range is from 1 to 4294967295.

Defaults

No default database is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SE	This command was introduced.

Usage Guidelines

In the DHCP snooping binding database, each database entry, also referred to 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 512 bindings.

When a switch learns new bindings or it loses bindings, the switch updates the entries in the database and in the binding file at a configured location. The frequency at which the database and the file are updated is based on a configurable delay, and the updates are batched. You can configure this delay by using the **ip dhcp snooping database write-delay** *seconds* global configuration command.

Use the **show ip dhcp snooping binding** privileged EXEC command to display only the dynamically configured bindings. Use the **show ip source binding** privileged EXEC command to display the dynamically and statically configured 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
gigabitethernet0/1 expiry 1000
```

You can verify your settings by entering the **show ip dhcp snooping binding** or the **show ip dhcp source binding** privileged EXEC command.

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP snooping on a VLAN.
show ip dhcp snooping binding	Displays the dynamically configured bindings in the DHCP snooping binding database and the configuration information.

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**]

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

flash:/*filename*	Specify that the database agent or the binding file is in the flash memory.
ftp://*user***:***password***@***host/filename*	Specify that the database agent or the binding file is on an FTP server.
http://*[[username:password]@]{hostname* | *host-ip}[/directory]/image-name*.**tar**	Specify that the database agent or the binding file is on an FTP server.
rcp://*user***@***host/filename*	Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server.
tftp://*host/filename*	Specify that the database agent or the binding file is on a TFTP server.
timeout *seconds*	Specify (in seconds) when to stop the database transfer process after the DHCP snooping binding database changes. The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an infinite duration.
write-delay *seconds*	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 from 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

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

The DHCP snooping binding database can have up to 8192 bindings.

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 capacity, 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 write bindings to the binding file at that URL for the first time.

Use the **ip dhcp snooping database flash:***/filename* command to save the DHCP snooping binding database in the stack master NVRAM. The database is not saved in a stack member NVRAM.

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 stack master 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
ip dhcp snooping	Enables DHCP snooping on a VLAN.
ip dhcp snooping binding	Configures the DHCP snooping binding database.
show ip dhcp snooping database	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 insertion is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

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** or **snmp-ifindex,** 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.

In Cisco IOS Release 12.1(19)EA1, the implementation for the option-82 subscriber identification changed from the previous release. The new option-82 format uses a different circuit ID and remote ID suboption, **vlan-mod-port**. The previous version uses the **snmp-ifindex** circuit ID and remote ID suboption.

You can select the previous option-82 format by using the **ip dhcp snooping information option format snmp-ifindex** global configuration command. When DHCP snooping is enabled globally, option-82 information (in the selected format) is only inserted on snooped VLANs.

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** privileged EXEC command.

Related Commands

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

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 configure the switch to drop these packets from the edge switch.

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

Release	Modification
12.1(22)EA3	This command was introduced.

Usage Guidelines

In Cisco IOS Release 12.1(22)EA3 and in Cisco IOS Release 12.2(25)SEA or later, 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** privileged EXEC command.

Related Commands

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

ip dhcp snooping information option format remote-id

Use the **ip dhcp snooping information option format remote-id** global configuration command on the switch to configure the option-82 remote-ID suboption. Use the **no** form of this command to configure the default remote-ID suboption.

ip dhcp snooping information option format remote-id [**string** *ASCII-string* | **hostname**]

no ip dhcp snooping information option format remote-id

Syntax Description

string *ASCII-string*	Specify a remote ID, using up to 63 ASCII characters (no spaces).
hostname	Specify the switch hostname as the remote ID.

Defaults

The switch MAC address is the remote ID.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

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, by default, the remote-ID suboption is the switch MAC address. You can use this command to configure either the switch hostname or a string of ASCII characters (but no spaces) to be the remote ID.

Note If the hostname exceeds 63 characters, it is truncated to 63 characters in the remote-ID configuration.

Examples

This example shows how to configure the option-82 remote-ID suboption:

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

Related Commands

Command	Description
ip dhcp snooping vlan information option format-type circuit-id string	Configures the option-82 circuit-ID suboption.
show ip dhcp snooping	Displays the DHCP snooping configuration.

ip dhcp snooping information option format snmp-ifindex

Use the **ip dhcp snooping information option format snmp-ifindex** global configuration command to select the **snmp-ifindex** alternative option-82 data format. Use the **no** form of this command to use the **vlan-mod-port** option-82 data format.

ip dhcp snooping information option format snmp-ifindex

no ip dhcp snooping information option format snmp-ifindex

Syntax Description

This command has no arguments or keywords.

Defaults

DHCP option-82 data insertion uses the **vlan-mod-port** format.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

If you have option 82 configured on the switch and you upgrade to Cisco IOS Release 12.1(19)EA1 or later, the option 82 configuration is not affected. However, when you enable DHCP snooping globally on the switch by using the **ip dhcp snooping global** configuration command, the **relay agent information option** configuration is disabled. This happens regardless of whether snooping is enabled on any VLANs. To provide for backward compatibility when using option 82 with DHCP snooping, you can select the previous option-82 format by using the **ip dhcp snooping information option format snmp-ifindex** global configuration command.

You can configure some switches in the network to continue using the previous option 82 format, and configure DHCP snooping on other switches in the network.

Option-82 information is only inserted on snooped VLANs.

Examples

This example shows how to enable DHCP option 82 data insertion in the snmp-ifindex format:

```
Switch(config)# ip dhcp snooping information option format snmp-ifindex
```

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

Related Commands

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

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

Syntax Description

rate	Number of DHCP messages an interface can receive per second. The range is 1 to 2048.

Defaults

DHCP snooping rate limiting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.
12.2(25)SE	The range was changed to 1 to 2048.

Usage Guidelines

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.

Examples

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** privileged EXEC command.

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	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

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

Configure as trusted ports that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports 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** privileged EXEC command.

Related Commands

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

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

Release	Modification
12.2(25)SE	This command was introduced.

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** privileged EXEC command.

Related Commands

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

ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** global configuration command to enable DHCP snooping on a VLAN. Use the **no** form of this command to disable DHCP snooping on a VLAN.

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

Syntax Description

vlan *vlan-range*	Specify a VLAN ID or 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

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch(config)# ip dhcp snooping vlan 10
```

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

Related Commands

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

ip dhcp snooping vlan information option format-type circuit-id string

Use the **ip dhcp snooping information option format-type circuit-id** interface configuration command on the switch 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* **information option format-type circuit-id string** *ASCII-string*

no ip dhcp snooping vlan *vlan* **information option format-type circuit-id string**

Syntax Description

vlan *vlan*	Specify the VLAN ID. The range is 1 to 4094.
string *ASCII-string*	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

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

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**. You can use this command to configure a string of ASCII characters to be the remote ID.

Note When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or the 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
customerABC-250-0-0
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

Note The **show** 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

Command	Description
ip dhcp snooping information option format remote-id	Configures the option-82 remote-ID suboption.
show ip dhcp snooping	Displays the DHCP snooping configuration.

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

Syntax Description

profile number	The IGMP profile number to be applied. The range is 1 to 4294967295.

Defaults

No IGMP filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or 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.

Examples

This example shows how to apply IGMP profile 22 to an interface.

```
Switch(config)# interface fastethernet0/1
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.

```
Switch# show running-config interface fastethernet0/1
Building configuration...

Current configuration : 124 bytes
!
interface FastEthernet0/1
 no ip address
 shutdown
 snmp trap link-status
 ip igmp filter 22
end
```

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.
show ip igmp profile	Displays the characteristics of the specified IGMP profile.
show running-config interface *interface-id*	Displays the running configuration on the switch interface, the IGMP profile (if any) that is applied to an interface. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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 return to the default settings.

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

Syntax Description

number	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
action deny	When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action.
action replace	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

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(19)EA1	The **action** {**deny**	**replace**} keywords were added.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups or configure the IGMP throttling action for routed ports, switch virtual interfaces (SVIs), or 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 and 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.

Examples

This example shows how to limit to 25 the number of IGMP groups that an interface can join.

```
Switch(config)# interface fastethernet0/1
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)# interface gigabitethernet0/1
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

Command	Description
show running-config interface *interface-id*	Displays the running configuration on the switch interface, including the maximum number of IGMP groups that an interface can join and the throttling action. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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*

Syntax Description

profile number	The IGMP profile number being configured. The range is 1 to 4294967295.

Defaults

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: specifies that matching addresses are denied; this is the default condition.
- **exit**: exits from igmp-profile configuration mode.
- **no**: negates a command or resets to its defaults.
- **permit**: specifies that matching addresses are permitted.
- **range**: 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.

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 terminal
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

Command	Description
ip igmp filter	Applies the IGMP profile to the specified interface.
show ip igmp profile	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*]

Syntax Description

vlan *vlan-id*	(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

Release	Modification
12.1(4)EA1	This command was introduced.

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.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	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**

Syntax Description

vlan *vlan-id*	(Optional) Enable IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
time	Interval time out in seconds. The range is 100 to 5000 milliseconds.

Defaults

The default timeout setting is 1000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEB	This command was introduced.

Usage Guidelines

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

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

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

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

The configuration is saved in NVRAM.

Examples

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

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

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

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

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

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	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

vlan *vlan-id*	(Optional) Enable IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
address *ip-address*	(Optional) 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.
max-response-time *response-time*	(Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
query-interval *interval-count*	(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.
tcn query [count *count* | **interval** *interval*]	(Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings: • **count** *count*—Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10. • **interval** *interval*—Set the TCN query interval time. The range is 1 to 255.
timer expiry	(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
version *version*	(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

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

```
Switch(config)# ip igmp snooping querier 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
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the IGMP snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	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

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

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

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP 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
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping source-only-learning age-timer

Use the **ip igmp snooping source-only-learning age-timer** global configuration command to enable and configure the aging time of the forward-table entries that the switch learns by using the source-only learning method. Use the **no** form of this command to return to the default setting.

ip igmp snooping source-only-learning age-timer *time*

no ip igmp snooping source-only-learning age-timer

Syntax Description

time	Aging time is seconds. The range is 0 to 2880 seconds. If you set *time* to 0, aging of the forward-table entries is disabled.

Defaults

The aging feature is enabled. The default is 600 seconds (10 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.

Usage Guidelines

In a source-only network, switch ports are connected to multicast source ports and multicast router ports. The switch ports are not connected to hosts that send IGMP join or leave messages.

The switch learns about IP multicast groups that alias with the reserved, destination, IP multicast addresses (in the range 224.0.0.xxx) from the IP multicast data stream by using the source-only learning method. The switch forwards traffic that aliases with these multicast addresses only to the multicast router ports. You cannot disable IP multicast-source-only learning for traffic that aliases with these multicast addresses.

The aging time only affects the forwarding-table entries that the switch learns by using the source-only learning method. If the aging time is too long or is disabled, the forwarding table is filled with unused multicast addresses that the switch learned by using source-only learning or by using the IGMP join messages. When the switch receives traffic for new IP multicast groups, it floods the packet to all ports in the same VLAN. This unnecessary flooding can impact switch performance.

To disable the aging of the forwarding-table entries, enter the **ip igmp snooping source-only-learning age-timer 0** global configuration command. If aging is disabled and you want to delete multicast addresses that the switch learned by using source-only-learning, re-enable aging of the forwarding-table entries. The switch can now age out the multicast addresses that were learned by the source-only learning method and that are not in use.

Examples

This example shows how to set the aging time as 1200 seconds (20 minutes):

```
Switch(config)# ip igmp snooping source-only-learning age-timer 1200
```

This example shows how to disable aging of the forward-table entries:

```
Switch(config)# ip igmp snooping source-only-learning age-timer 0
```

You can verify your settings by entering the **show running-config | include source-only-learning** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
show running-config | include source-only-learning	Displays the configuration information running on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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**}

Syntax Description

flood query count *count*	Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10.
query solicit	Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event.

Defaults

The TCN flood query count is 2.

The TCN query solicitation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEB	This command was introduced.

Usage Guidelines

Use **ip igmp snooping tcn flood query count** 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 **ip igmp snooping tcn flood query count** command, the flooding stops after receiving one 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 and to speed the process of recovering from the flood mode caused during a TCN event.

Examples

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.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping tcn flood	Specifies flooding on an interface as the IGMP snooping spanning-tree TCN behavior.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

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

Release	Modification
12.2(25)SEB	This command was introduced.

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)# interface gigabitethernet0/2
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
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping tcn	Configures the IGMP TCN behavior on the switch.
show ip igmp snooping	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**

Syntax Description

vlan-id	Enable IGMP snooping and the Immediate-Leave feature on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Defaults

IGMP immediate-leave processing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

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
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

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

vlan-id	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.
interface *interface-id*	Specify the next-hop interface to the multicast router. The keywords have these meanings: • **fastethernet** *interface number*—a Fast Ethernet IEEE 802.3 interface. • **gigabitethernet** *interface number*—a Gigabit Ethernet IEEE 802.a interface. • **port-channel** *interface number*—a channel interface. The range is 0 to 64.
learn {**cgmp** | **pim-dvmrp**}	Specify the multicast router learning method. The keywords have these meanings: • **cgmp**—Set the switch to learn multicast router ports by snooping on Cisco Group Management Protocol (CGMP) packets. • **pim-dvmrp**—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.

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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

The CGMP learn method is useful for reducing control traffic.

The configuration is saved in NVRAM.

Examples

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

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

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

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

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

Related Commands

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

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

vlan-id	Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
ip-address	Add a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specify the interface of the member port. The keywords have these meanings: • **fastethernet** *interface number*—a Fast Ethernet IEEE 802.3 interface. • **gigabitethernet** *interface number*—a Gigabit Ethernet IEEE 802.a interface. • **port-channel** *interface number*—a channel interface. The range is 0 to 64.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

The configuration is saved in NVRAM.

Examples

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

```
Switch(config)# ip igmp snooping vlan 1 static 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
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

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

mac-address	Specify a MAC address.
vlan *vlan-id*	Specify a VLAN number. The range is from 1 to 4094.
ip-address	Specify an IP address.
interface *interface-id*	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

Release	Modification
12.2(25)SEA	This command was introduced.

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
gigabitethernet0/1
```

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
gigabitethernet0/1
Switch(config)# ip source binding 0001.1357.0007 vlan 1 172.20.50.30 interface
gigabitethernet0/1
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

Related Commands

Command	Description
ip verify source	Enables IP source guard on an interface.
show ip source binding	Displays the IP source bindings on the switch.
show ip verify source	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. Use the **no** form of this command to return to the default setting.

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

This command is available only when your switch is running the cryptographic (encrypted) software image.

Syntax Description

1	(Optional) Configure the switch to run SSH version 1 (SSHv1).
2	(Optional) Configure the switch to run SSH version 2 (SSHv1).

Defaults

The default version is the latest SSH version supported by the SSH client.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

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
show ip ssh	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features** > **Secure Shell Commands**.
show ssh	Displays the status of the SSH server. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features** > **Secure Shell Commands**.

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 [p**ort-security**]

no ip verify source

Syntax Description

port-security	(Optional) Enable IP source guard with IP and MAC address filtering. If you do not enter the **port-security** keyword, IP source guard with IP address filtering is enabled.

Defaults

IP source guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP and MAC address filtering, use the **ip verify source port-security** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering:

```
Switch(config-if)# ip verify source
```

This example shows how to enable IP source guard with source IP and MAC address filtering:

```
Switch(config-if)# ip verify source port-security
```

You can verify your settings by entering the **show ip source binding** privileged EXEC command.

Related Commands

Command	Description
ip source binding	Configures static bindings on the switch.
show ip verify source	Displays the IP source guard configuration on the switch or on a specific interface.

ip vrf (global configuration)

Use the **ip-vrf** global configuration command to configure a Virtual Private Network (VPN) routing/forwarding (VRF) routing table and to enter VRF configuration mode. Use the **no** form of this command to remove a VRF routing table and to return to global configuration mode.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Note The switch supports multi-VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices. You must have the IP services image, formerly known as the enhanced multilayer image (EMI), installed on your switch to configure multi-VRF CE.

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

No VRFs are defined.

No import or export lists are associated with a VRF.

No route maps are associated with a VRF.

The maximum number of routes in a VRF is 8000 for Fast Ethernet switches and 12000 for Gigabit Ethernet switches.

Command Modes

Global configuration or router configuration

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

Usage Guidelines

Entering the **ip vrf** command enables the VRF configuration mode. These configuration commands are available:

- **default**: set a command (description, export, import, maximum routes, route-target) to its default setting.
- **description**: describes the VRF (up to 80 characters).
- **exit**: exits VRF configuration mode and returns to global configuration mode.
- **export map** *route-map*: set a route-map to be used as an export route map for the VRF.
- **import map** *route-map*: set a route-map to be used as an import route map for the VRF.
- **maximum routes** *limit* {*warn threshold* | **warn-only**}: limit the maximum number of routes in a VRF to prevent a PE router from importing too many routes. The limits are from 1 to 4294967295; the threshold is a percentage of the limit, from 1 to 100.
- **no**: negate a command or return to its default setting.

- **rd**: specify Route Distinguisher as either an autonomous system-relative composed of an autonomous system (AS) number and an arbitrary number, or as an IP-address-relative composed of an IP address and an arbitrary number.
  - 16-bit AS number: 32-bit number (for example, 101:3)
  - 32-bit IP address: 16-bit number (for example, 192.168.122.15:1.)
- **route-target** {**import** | **export** | **both**} *route-target-ext-community*: specify Target VPN Extended Communities. You can specify the Target for export, import, or both.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Use an import route map when an application requires finer control over the routes imported into a VRF than that provided by the import and export extended communities configured for the importing and exporting VRF. The **import map** command associates a route map with the specified VRF. You can filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route, by using a route map. The route map might deny access to selected routes from a community that is on the import list.

If you set a maximum routes threshold, the switch rejects routes when the threshold limit is reached. If you enter **warn-only**, the switch creates a syslog error message when the maximum number of VRF routes exceeds the allowed limit, but additional routes are still allowed

A route distinguisher (RD) creates routing and forwarding tables and specifies the default route distinguisher for a VPN. A route distinguisher must be configured for a VRF to be functional. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

The route target specifies a target VPN extended community. Like a route-distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number.

The **ip vrf** vrf-name command creates a VRF routing table and a Cisco Express Forwarding (CEF) forwarding table, both named *vrf-name*. Associated with these tables is the default route distinguisher value *route-distinguisher*.

Examples

This example shows how to create the VRF named *vpn1*, enter VRF configuration mode, and import a route map to the VRF:

```
Switch(config)# ip vrf vpn1
Switch(config-vrf)# rd 100:2
Switch(config-vrf)# route-target both 100:2
Switch(config-vrf)# route-target import 100:1
```

Related Commands

Command	Description
ip vrf (interface configuration)	Associate a VRF routing table or a route map with an interface.
show ip route vrf	Displays the IP routing table associated with a VRF. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2**.
show ip vrf	Displays display the set of defined VRFs and associated interfaces. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2**.

ip vrf (interface configuration)

Use the **ip-vrf** interface configuration command to associate a Virtual Private Network (VPN) routing/forwarding (VRF) routing table or a route map with an interface. Use the **no** form of this command to disassociate the VRF routing table or route map.

ip vrf {**forwarding** *table-name* | **sitemap** *route-map-name*}

no ip vrf {**forwarding** *table-name* | **sitemap** *route-map-name*}

Note The switch supports multi-VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices. You must have the IP services image, formerly known as the enhanced multilayer image (EMI), installed on your switch to configure multi-VRF CE.

Syntax Description

forwarding *table-name*	Specify a VRF forwarding table name for the interface.
sitemap *route-map-name*	Specify a VRF route-map for routes received from this site.

Defaults

The default for an interface is the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

Usage Guidelines

Use the **ip vrf forwarding** command to associate an interface with a VRF. Executing this command on an interface removes the IP address. You must reconfigure the IP address.

Examples

This example shows how to link the VRF named *vpn1* to an interface:

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
ip vrf (global configuration)	Configures a VRF routing table.
ip route vrf	Establishes static routes for a VRF. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2**.
show ip route vrf	Displays the IP routing table associated with a VRF. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2**.
show ip vrf	Displays display the set of defined VRFs and associated interfaces. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2**.

l2protocol-tunnel

Use the **l2protocol-tunnel** interface configuration command to enable tunneling of Layer 2 protocols on an access or IEEE 802.1Q tunnel port or on a port channel. You can enable tunneling for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. You can also enable point-to-point tunneling for Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or UniDirectional Link Detection (UDLD) packets. Use the **no** form of this command to disable tunneling on the interface.

l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] | [**shutdown-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] *value*] | [**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]] *value*]

no l2protocol-tunnel [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]] | [**shutdown-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]] | [**drop-threshold** [**cdp** | **stp** | **vtp**] [**point-to-point** [**pagp** | **lacp** | **udld**]]]

Syntax Description

l2protocol-tunnel	Enable point-to-multipoint tunneling of CDP, STP, and VTP packets.
cdp	(Optional) Enable tunneling of CDP, specify a shutdown threshold for CDP, or specify a drop threshold for CDP.
stp	(Optional) Enable tunneling of STP, specify a shutdown threshold for STP, or specify a drop threshold for STP.
vtp	(Optional) Enable tunneling or VTP, specify a shutdown threshold for VTP, or specify a drop threshold for VTP.
point-to-point	(Optional) Enable point-to point tunneling of PAgP, LACP, and UDLD packets.
pagp	(Optional) Enable point-to-point tunneling of PAgP, specify a shutdown threshold for PAgP, or specify a drop threshold for PAgP.
lacp	(Optional) Enable point-to-point tunneling of LACP, specify a shutdown threshold for LACP, or specify a drop threshold for LACP.
udld	(Optional) Enable point-to-point tunneling of UDLD, specify a shutdown threshold for UDLD, or specify a drop threshold for UDLD.
shutdown-threshold	(Optional) Set a shutdown threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface is shut down.
drop-threshold	(Optional) Set a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
value	Specify a threshold in packets per second to be received for encapsulation before the interface shuts down, or specify the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.

Defaults

The default is that no Layer 2 protocol packets are tunneled.

The default is no shutdown threshold for the maximum number of Layer 2 protocol packets.

The default is no drop threshold for the maximum number of Layer 2 protocol packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The **drop-threshold** keywords was added.
12.1(19)EA1	The **point-to-point**, **pagp**, **lacp**, and **udld** keywords were added.

Usage Guidelines

You must enter this command, with or without protocol types, to tunnel Layer 2 packets.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well-known Cisco multicast address for transmission across the network. When the packets reach their destination, the well-known MAC address is replaced by the Layer 2 protocol MAC address.

You can enable Layer 2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols.

In a service-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When protocol tunneling is enabled on the service-provider switch for PAgP or LACP, remote customer switches receive the protocol data units (PDUs) and can negotiate automatic creation of EtherChannels.

To enable tunneling of PAgP, LACP, and UDLD packets, you must have a point-to-point network topology. To decrease the link-down detection time, you should also enable UDLD on the interface when you enable tunneling of PAgP or LACP packets.

You can enable point-to-point protocol tunneling for PAgP, LACP, and UDLD individually or for all three protocols.

Caution PAgP, LACP, and UDLD tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

Enter the **shutdown-threshold** keyword to control the number of protocol packets per second that are received on an interface before it shuts down. When no protocol option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

When the shutdown threshold is reached, the interface is error-disabled. If you enable error recovery by entering the **errdisable recovery cause l2ptguard** global configuration command, the interface retries the operation again when all the causes have timed out. If the error recovery mechanism is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

Enter the **drop-threshold** keyword to control the number of protocol packets per second that are received on an interface before it drops packets. When no protocol option is specified with a keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a shutdown threshold, the drop-threshold value must be less than or equal to the shutdown-threshold value.

When the drop threshold is reached, the interface drops Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

The configuration is saved in NVRAM.

Note For more information about Layer 2 protocol tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable protocol tunneling for CDP packets and to set the shutdown threshold to 50 packets per second:

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

This example shows how to enable protocol tunneling for STP packets and to set the drop threshold to 400 packets per second:

```
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel drop-threshold stp 400
```

This example shows how to enable point-to-point protocol tunneling for PAgP and UDLD packets and to set the PAgP drop threshold to 1000 packets per second:

```
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

Related Commands

Command	Description
l2protocol-tunnel cos	Configures a class of service (CoS) value for all tunneled Layer 2 protocol packets.
show errdisable recovery	Displays error-disabled recovery timer information.
show l2protocol-tunnel	Displays information about ports configured for Layer 2 protocol tunneling, including port, protocol, class of service (CoS), and thresholds.

l2protocol-tunnel cos

Use the **l2protocol-tunnel cos** global configuration command to configure class of service (CoS) value for all tunneled Layer 2 protocol packets. Use the **no** form of this command to return to the default setting.

l2protocol-tunnel cos *value*

no l2protocol-tunnel cos

Syntax Description

value	Specify CoS priority value for tunneled Layer 2 protocol packets. The range is 0 to 7, with 7 being the highest priority.

Defaults

If a CoS value is configured for data packets for the interface, the default is to use this CoS value for tunneled Layer 2 protocol packets. If no CoS value is configured for the interface, the default is 5.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

When enabled, the tunneled Layer 2 protocol packets use this CoS value.

The value is saved in NVRAM.

Examples

This example shows how to configure a Layer-2 protocol-tunnel CoS value of 7:

```
Switch(config)# l2protocol-tunnel cos 7
```

Related Commands

Command	Description
show l2protocol-tunnel	Displays information about ports configured for Layer 2 protocol tunneling, including CoS.

lacp port-priority

Use the **lacp port-priority** interface configuration command to set 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-value*

no lacp port-priority

Syntax Description

priority-value	Port priority for LACP. The range is 1 to 65535.

Defaults

The default priority value is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

This command only takes effect on EtherChannel interfaces that are already configured for LACP.

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 more information about configuring LACP on physical interfaces, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Examples

This example shows set the port priority for LACP:

```
Switch(config)# lacp port-priority 32764
```

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

Related Commands

Command	Description
lacp system-priority	Globally sets the LACP priority.

lacp system-priority

Use the **lacp system-priority** global configuration command to set the system priority for Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

lacp system-priority *priority-value*

no lacp system-priority

Syntax Description

priority-value	System priority for LACP. The range is 1 to 65535.

Defaults

The default priority value is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

The **lacp system-priority** 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 interfaces, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Examples

This example shows how to set the system priority for LACP:

```
Switch(config)# lacp system-priority 32764
```

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

Related Commands

Command	Description
lacp port-priority	Sets the LACP priority for a specific port.

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 flash:*filename* [*max-file-size*] [*min-file-size*] [*severity-level-number* | *type*]

no logging file flash:*filename* [*severity-level-number* | *type*]

Syntax Description

flash:*filename*	The path and name of the file that contains the log messages.
max-file-size	(Optional) Specify the maximum logging file size. The range is 4096 to 2147483647.
min-file-size	(Optional) Specify the minimum logging file size. The range is 1024 to 2147483647.
severity-level-number	(Optional) Specify the logging severity level. The range is 0 to 7. See the *type* option for the meaning of each level.
type	(Optional) Specify the logging type. These keywords are valid: • **emergencies**—System is unusable (severity 0). • **alerts**—Immediate action needed (severity 1). • **critical**—Critical conditions (severity 2). • **errors**—Error conditions (severity 3). • **warnings**—Warning conditions (severity 4). • **notifications**—Normal but significant messages (severity 5). • **information**—Information messages (severity 6). • **debugging**—Debugging messages (severity 7).

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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The log file is stored in ASCII text format. You can use the **more** privileged EXEC command to display its contents.

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

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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 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*]

Syntax Description

name	Specify a named MAC access list.
in	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

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

You can apply MAC ACLs only to ingress Layer 2 interfaces. You cannot apply MAC ACLs to Layer 3 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 cannot apply more than one MAC ACL to a 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.

You cannot apply a MAC ACL (or IP ACL) to a Layer 2 interface on a switch that has an input Layer 3 ACL or a VLAN map applied to it. If a switch has a MAC ACL or IP ACL applied to a Layer 2 interface, you cannot apply an IP ACL to an input Layer 3 interface on that switch, and you cannot apply a VLAN map to any of the switch VLANs.

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 action.

If the specified ACL does not exist, the switch forwards all packets.

Note 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)# interface fastethernet0/1
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 view configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
show access-lists	Displays the ACLs configured on the switch.
show mac access-group	Displays the MAC ACLs configured on the switch.
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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*

Syntax Description

name	Assign a name to the MAC extended access list.

Defaults

By default, there are no MAC access lists created.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

MAC named extended lists are used with VLAN maps and class maps.

You should use this command (and not the **access-list** global configuration command) for defining Layer 2 access lists.

Entering the **mac access-list extended** command enables the MAC-access list configuration mode. These configuration commands are available:

- **default**: sets a command to its default.
- **deny**: specifies packets to reject. For more information, see the **deny** MAC-access list configuration command.
- **exit**: exits from MAC-access list configuration mode.
- **no**: negates a command or sets its defaults.
- **permit**: specifies packets to forward. For more information, see the **permit** command.

Note For more information about MAC extended access lists, see the software configuration guide for this release.

Examples

This example shows how to create a MAC named extended access list named *mac1* and to enter extended MAC access list configuration mode:

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

This example shows how to delete MAC named extended access list *mac1*:

```
Switch(config)# no mac access-list extended mac1
```

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

Related Commands

Command	Description
deny **permit**	Configures the MAC ACL (in extended MAC-access list configuration mode).
show access-lists	Displays the access lists configured on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

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*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **mac address-table aging-time** command replaces the **mac-address-table aging-time** command (with the hyphen).

Syntax Description

0	Aging is disabled. Static address entries are never aged or removed from the table.
10-100000	Aging time in seconds. The range is 10 to 1000000 seconds.
vlan *vlan-id*	(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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **mac-address-table aging-time** command was replaced by the **mac address-table aging-time** command.

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.

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.

Related Commands

Command	Description
show mac address-table aging-time	Displays the MAC address table aging time for all VLANs or the specified VLAN.

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 [**history-size** *value*] | [**interval** *value*]

no mac address-table notification [**history-size** | **interval**]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **mac address-table notification** command replaces the **mac-address-table notification** command (with the hyphen).

Syntax Description

history-size *value*	(Optional) Configure the maximum number of entries in the MAC notification history table. The range is 1 to 500 entries.
interval *value*	(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.

Defaults

By default, the MAC address notification feature is disabled.

The default trap interval value is 1 second.

The default number of entries in the history table is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(11)EA1	The **mac-address-table notification** command was replaced by the **mac address-table notification** command.

Usage Guidelines

The MAC address notification 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 notifications are generated only for dynamic and secure MAC addresses. Events are not generated for self addresses, multicast addresses, or other static addresses.

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 feature by using the **mac address-table notification** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification** global configuration command.

Examples

This example shows how to enable the MAC address-table notification feature, set the interval time to 60 seconds, and set the history-size to 100 entries:

```
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table notification	Displays the MAC address notification settings on all interfaces or on the specified interface.
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.
snmp trap mac-notification	Enables the SNMP MAC notification 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*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **mac address-table static** command replaces the **mac-address-table static** command (with the hyphen).

Syntax Description

mac-addr	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.
vlan *vlan-id*	Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
interface *interface-id*	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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **mac-address-table static** command was replaced by the **mac address-table static** command.

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
gigabitethernet0/1
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

Related Commands

Command	Description
show mac address-table static	Displays static MAC address table entries only.

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*

Syntax Description

mac-addr	Unicast source or destination MAC address. Packets with this MAC address are dropped.
vlan *vlan-id*	Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.

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

Release	Modification
12.1(19)EA1	This command was introduced.

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
show mac address-table static	Displays only static MAC address table entries.

macro apply

Use the **macro apply** interface configuration command to apply a macro to an interface or to apply and trace a macro configuration on an interface.

macro {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Syntax Description

apply	Apply a macro to the specified interface.
trace	Use the **trace** keyword to apply a macro to an interface and to debug the macro.
macro-name	Specify the name of the macro.
parameter *value*	(Optional) Specify unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.
12.1(20)EA1	The **parameter** *value* keywords were added.

Usage Guidelines

You can use the **macro trace** *macro-name* interface configuration command to apply and show the macros running on an interface or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the interface.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the interface.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro apply** *macro-name* **?** command to view a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on an interface:

- Display all macros on the switch by using the **show parser macro** user EXEC command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* user EXEC command.
- Keywords that begin with **$** mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

  The Cisco-default macros use the **$** character to help identify required keywords. There is no restriction on using the **$** character to define keywords when you create a macro.

When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the **show running-configuration interface** *interface-id* user EXEC command.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.

You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* interface configuration command.

Examples

After you have created a macro by using the **macro name** global configuration command, you can apply it to an interface. This example shows how to apply a user-created macro called **duplex** to an interface:

```
Switch(config-if)# macro apply duplex
```

To debug a macro, use the **macro trace** interface configuration command to find any syntax or configuration errors in the macro as it is applied to an interface. This example shows how troubleshoot the user-created macro called **duplex** on an interface:

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

This example shows how to display the Cisco-default **cisco-desktop** macro and how to apply the macro and set the access VLAN ID to 25 on an interface:

```
Switch# show parser macro cisco-desktop
------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default

# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
switchport port-security maximum 1

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
------------------------------------------------------------
Switch#
Switch# configure terminal
Switch(config)# interface fastethernet0/4
Switch(config-if)# macro apply cisco-desktop $AVID 25
```

Related Commands

Command	Description
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro description

Use the **macro description** interface configuration command to enter a description about which macros are applied to an interface. Use the **no** form of this command to remove the description.

macro description *text*

no macro description *text*

Syntax Description

description *text*	Enter a description about the macros that are applied to the specified interface.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with an interface. When multiple macros are applied on a single interface, the description text will be from the last applied macro.

This example shows how to add a description to an interface:

```
Switch(config-if)# macro description duplex settings
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro global

Use the **macro global** global configuration command to apply a macro to a switch or to apply and trace a macro configuration on a switch.

macro global {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Syntax Description

apply	Apply a macro to the switch.
trace	Use the **trace** keyword to apply a macro to a switch and to debug the macro.
macro-name	Specify the name of the macro.
parameter *value*	(Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(20)EA2	This command was introduced.

Usage Guidelines

You can use the **macro trace** *macro-name* global configuration command to apply and to show the macros running on a switch or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

There are Cisco-default Smartports macros embedded in the switch software. You can display these macros and the commands they contain by using the **show parser macro** user EXEC command.

Follow these guidelines when you apply a Cisco-default Smartports macro on a switch:

- Display all macros on the switch by using the **show parser macro** user EXEC command. Display the contents of a specific macro by using the **show parser macro name** *macro-name* user EXEC command.
- Keywords that begin with **$** mean that a unique parameter value is required. Append the Cisco-default macro with the required values by using the **parameter** *value* keywords.

  The Cisco-default macros use the **$** character to help identify required keywords. There is no restriction on using the **$** character to define keywords when you create a macro.

When you apply a macro to a switch, the macro name is automatically added to the switch. You can view the applied commands and macro names by using the **show running-configuration** user EXEC command.

You can delete a global macro-applied configuration on a switch only by entering the **no** version of each command contained in the macro.

Examples

After you have created a new macro by using the **macro name** global configuration command, you can apply it to a switch. This example shows how display the **snmp** macro and how to apply the macro and set the host name to test-server and set the IP precedence value to 7:

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

----------------------------------------------------
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global trace** global configuration command to find any syntax or configuration errors in the macro when it is applied to a switch. In this example, the **ADDRESS** parameter value was not entered, causing the `snmp-server host` command to fail while the remainder of the macro is applied to the switch:

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro global description

Use the **macro global description** global configuration command to enter a description about the macros that are applied to the switch. Use the **no** form of this command to remove the description.

macro global description *text*

no macro global description *text*

Syntax Description

description *text*	Enter a description about the macros that are applied to the switch.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(20)EA2	This command was introduced.

Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.

This example shows how to add a description to a switch:

```
Switch(config)# macro global description udld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro name	Creates a macro.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro name

Use the **macro name** global configuration command to create a configuration macro. Use the **no** form of this command to delete the macro definition.

macro name *macro-name*

no macro name *macro-name*

Syntax Description

macro-name	Name of the macro.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)EA1	This command was introduced.
12.1(20)EA2	The help string **# macro keywords** was added.

Usage Guidelines

A macro can contain up to 3000 characters. Enter one macro command per line. Use the **@** character to end the macro. Use the **#** character at the beginning of a line to enter comment text within the macro.

You can define mandatory keywords within a macro by using a help string to specify the keywords. Enter **# macro keywords** *word* to define the keywords that are available for use with the macro. You can enter up to three help string keywords separated by a space. If you enter more than three macro keywords, only the first three are shown.

Macro names are case sensitive. For example, the commands **macro name Sample-Macro** and **macro name sample-macro** will result in two separate macros.

When creating a macro, do not use the **exit** or **end** commands or change the command mode by using **interface** *interface-id*. This could cause commands that follow **exit**, **end**, or **interface** *interface-id* to execute in a different command mode.

The **no** form of this command only deletes the macro definition. It does not affect the configuration of those interfaces on which the macro is already applied. You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* interface configuration command. Alternatively, you can create an *anti-macro* for an existing macro that contains the **no** form of all the corresponding commands in the original macro. Then apply the anti-macro to the interface.

You can modify a macro by creating a new macro with the same name as the existing macro. The newly created macro overwrites the existing macro but does not affect the configuration of those interfaces on which the original macro was applied.

Examples

This example shows how to create a macro that defines the duplex mode and speed:

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

This example shows how create a macro with **# macro keywords**:

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

This example shows how to display the mandatory keyword values before you apply the macro to an interface:

```
switch(config)# interface fa0/1
switch(config-if)# macro apply test ?
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID ?
  WORD  Value of first keyword to replace

Switch(config-if)# macro apply test $VLANID 2
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID 2 $MAX ?
  WORD  Value of second keyword to replace
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
show parser macro	Displays the macro definition for all macros or for the specified macro.

match (access-map configuration)

Use the **match** access-map configuration command to set the VLAN map to match packets against one or more access lists. Use the **no** form of this command to remove the match parameters.

match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

Syntax Description

ip address	Set the access map to match packets against an IP address access list.
mac address	Set the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Defaults

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

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

Related Commands

Command	Description
access-list	Configures a standard numbered ACL. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
action	Specifies the action to be taken if the packet matches an entry in an access control list (ACL).
ip access list	Creates a named access list. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
mac access-list extended	Creates a named MAC address access list.
match (access-map configuration)	Defines the match conditions for a VLAN map.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Creates a VLAN access map.

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* | **class-map** *class-map-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **vlan** *vlan-list*}

no match {**access-group** *acl-index-or-name* | **class-map** *class-map-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **vlan** *vlan-list*}

Syntax Description

access-group *acl-index-or-name*	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.
class-map *class-map-name*	Name of predefined class map for classification that is performed on a per-port per-VLAN basis.
ip dscp *dscp-list*	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.
ip precedence *ip-precedence-list*	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
vlan *vlan-list*	List of VLANs to match against incoming packets. You can enter up to 30 VLAN IDs. Use a hyphen for a range of VLANs. A VLAN range is counted as two VLAN IDs. Use a space to separate individual VLANs. The range is 1 to 4094.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **class-map** and **vlan** keywords were added.

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.

To define packet classification on a per-port per-VLAN basis, follow these guidelines:

- You must use the **match-all** keyword with the **class-map** global configuration command to imply the Logical-AND of all matching statements under this class map.
- Per-port per-VLAN classification is a per-port feature and does not work on redundant links. It is supported only on an ingress port configured as a trunk or as a static-access port.
- The class map must have two **match** commands in this order: one **match vlan** *vlan-list* class-map configuration command and one **match class-map** *class-map-name* class-map configuration command. The class map specified in the **match class-map** *class-map-name* command must be predefined and cannot contain the **match vlan** *vlan-list* and the **match class-map** *class-map-name* commands.
- You cannot configure both port-based classification and VLAN-based classification at the same time. When you enter the **match vlan** *vlan-list* command, the class map becomes per-port per-VLAN based. If you configure a policy map that contains both port-based and VLAN-based class maps, the switch rejects the policy map when you attach it to an interface.
- Within a policy map, when you use the **match vlan** *vlan-list* command, all other class maps must use the **match vlan** *vlan-list* command.
- If you want to modify the VLAN list, first remove the previous configuration in the class map by using the **no match vlan** *vlan-list* command and the **no match class-map** *class-map-name* command. Then reconfigure the class map, and specify the new VLAN list. If the policy map is attached to an interface and you modify the class map by using any other method, the policy map detaches from the interface.

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.

You cannot attach policy maps that contain these elements to an egress interface by using the **service-policy** interface configuration command:

- **set** or **trust** policy-map class configuration commands. Instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

The only match criterion in a policy map that can be attached to an egress interface is the **match ip dscp** *dscp-list* class-map configuration command.

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 with *acl1*:

```
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 acl1
Switch(config-cmap)# exit
```

This example shows how to configure a class map called *dscp_class* whose match criterion is to match IP DSCP 9. A second class map, called *vlan_class*, matches traffic on VLANs 10, 20 to 30, and 40 to class map *dscp_class*:

```
Switch(config)# class-map match-any dscp_class
Switch(config-cmap)# match ip dscp 9
Switch(config-cmap)# exit
Switch(config)# class-map match-all vlan_class
Switch(config-cmap)# match vlan 10 20-30 40
Switch(config-cmap)# match class-map dscp_class
Switch(config-cmap)# exit
```

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

mls aclmerge delay

Use the **mls aclmerge delay** global configuration command to adjust the time required for access control list (ACL) configuration to be stable before the system performs ACL merges and ternary content addressable memory (TCAM) updates. Use the **no** form of this command to return to the default setting.

mls aclmerge delay *delay-time*

no mls aclmerge delay

Syntax Description

delay-time	The time in milliseconds that the system requires ACL configuration to be stable before it performs an ACL merge. The range is 0 to 3000.

Defaults

The default time is 3000 milliseconds (3 seconds).

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

Usage Guidelines

Because ACL merges take a significant amount of time, if the configuration of security ACLs on the system is changing rapidly, the software postpones ACL merges and TCAM updates until the configuration is no longer changing. By default, if a new security ACL-related configuration change is made within 3000 milliseconds of a previous change, the merge is postponed. ACL-related configuration changes include applying ACLs to interfaces or making changes to ACLs or VLAN maps that are already applied to interfaces. All postponed merges and TCAM updates are performed by a background process after the configuration has been stable for 3000 milliseconds. A configuration is stable if no changes are being made that affect information stored in the TCAM.

Entering the **mls aclmerge delay** command allows the merge delay to be adjusted to less than 3 seconds. Setting the delay to 0 causes all merges to be performed immediately as the configuration is changed.

New settings affect all ACL configuration changes made after the command is entered. If the configuration is saved to the startup configuration file, when the switch boots up, the merge settings do not take affect until after the complete saved configuration file is read. This allows initial configuration to proceed efficiently.

Examples

This example shows how to change the merge delay to be 2000 milliseconds (2 seconds):

```
Switch(config)# mls aclmerge delay 2000
```

This example shows how to set the merge to be performed immediately:

```
Switch(config)# mls aclmerge delay 0
```

You can verify the ACL merge setting by entering the **show running-config | include mls aclmerge delay** privileged EXEC command.

Related Commands

Command	Description
access-list {**deny** | **permit**}	Configures a standard numbered ACL. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
action (access map configuration)	Defines or modifies the action for the VLAN access map entry.
ip access-group	Applies an IP access list to a Layer 2 or Layer 3 interface.
ip access-list	Configures a named access list. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
mac access-group	Applies a MAC access list to a Layer 2 interface.
match (access-map configuration)	Defines the match conditions for a VLAN map.
show running-config | include mls aclmerge delay	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
vlan access-map	Creates a VLAN access map or enters access-map configuration mode.
vlan filter	Applies a VLAN map to one or more VLANs.

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

Syntax Description

This command has no arguments or keywords.

Defaults

QoS is disabled. Table 2-5 shows the default QoS settings when QoS is disabled.

Table 2-5 Default QoS Configuration when QoS is Disabled

Port Type	QoS State	Egress traffic (DSCP[1] and CoS[2] Value)	Queue	Queue Weights	Tail-drop Thresholds	CoS Mapping to Queue
Gigabit-capable Ethernet ports	Disabled	Pass through.	All the queue RAM is allocated to queue 1 (no expedite queue).	–	100%, 100% WRED[3] is disabled.	All CoS values map to queue 1.
10/100 Ethernet ports	Disabled	Pass through.	Each of the eight minimum-reserve levels have a buffer size of 100 packets. The queue selects the level.	–	–	All CoS values map to queue 1.

1. Differentiated Services Code Point
2. Class of service
3. Weighted Random Early Detection

When 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).

Table 2-6 shows the default QoS settings when QoS is enabled.

Table 2-6 Default QoS Configuration when QoS is Enabled

Port Type	QoS State	Egress traffic (DSCP and CoS Value)	Queue	Queue Weights	Tail-drop Thresholds	CoS Mapping to Queue
Gigabit-capable Ethernet ports	Enabled (no policing)	DSCP=0 CoS=0 (0 means best-effort delivery.)	Four queues are available (no expedite queue).	Each queue has the same weight.	100%, 100% WRED is disabled.	0, 1: queue 1 2, 3: queue 2 4, 5: queue 3 6, 7: queue 4
10/100 Ethernet ports	Enabled (no policing)	DSCP=0 CoS=0 (0 means best-effort delivery.)	Each of the eight minimum-reserve levels have a buffer size of 100 packets. The queue selects the level.	Each queue has the same weight.	–	0, 1: queue 1 2, 3: queue 2 4, 5: queue 3 6, 7: queue 4

When QoS is enabled, the default trust state on all ports is untrusted.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

QoS must be globally enabled to use QoS classification, policing, mark down or drop, and queueing features. You can create a policy-map and attach it to a port before executing the **mls qos** command. However, until you enter the **mls qos** command, QoS processing is disabled.

You must disable IEEE 802.3x flow control on all ports before enabling QoS on the switch. To disable it, use the **flowcontrol receive off** and **flowcontrol send off** interface configuration commands.

Note If QoS is disabled and you enter the **mls qos** global configuration command, this message appears:
`QoS:ensure flow-control on all interfaces are OFF for proper operation.`

When QoS is enabled without any further configuration, ingress traffic is classified to best-effort without any policing. DSCP and CoS values carried in packets are rewritten to 0. For the egress direction, all four queues are configured with same weighted round robin (WRR) weights, and all the packets (that have been classified as best-effort traffic) are placed at the queue mapped to CoS value equal to 0.

QoS features at the ingress port include traffic classification (by class map, packet DSCP/CoS, or port DSCP/CoS), policing, and possibly marking-down or dropping out-of-profile packets. At the egress port, traffic can be also classified (by packet DSCP or CoS assigned at the ingress port), policed, and possibly marked down or dropped. If not dropped, the packet is placed in one of four queues, which can be configured with tail-drop or WRED threshold parameters.

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.

When QoS is disabled, ingress traffic is switched in pass-through mode, which means packets are switched without any rewrites and are classified to best effort without any policing. No ingress and egress policers are configured. All CoS values for egress traffic are mapped to queue 1.

Toggling the QoS status of the switch with this command modifies (reallocates) the sizes of the queues. During the queue size modification, the switch is in a *halt* mode and drops packets for a short period.

Examples

This example shows how to disable flow control on all interfaces and then enable QoS on the switch:

```
Switch(config)# interface range gigabitethernet0/1 -12
Switch(config-if)# flowcontrol receive off
Switch(config-if-range)# flowcontrol send off
Switch(config-if-range)# exit
Switch(config)# mls qos
```

This example shows how to disable all QoS processing on the switch:

```
Switch(config)# no mls qos
```

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

Related Commands

Command	Description
flowcontrol	Sets the receive or send flow-control value for an interface.
mls qos min-reserve	Configures the minimum-reserve levels (segments) on 10/100 Ethernet ports.
show mls qos	Displays QoS information.
wrr-queue bandwidth	Assigns WRR weights to the four egress queues.
wrr-queue min-reserve	Assigns a minimum-reserve level to an egress queue on a 10/100 Ethernet port.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.
wrr-queue threshold	Assigns tail-drop threshold percentages to an egress queue of a Gigabit-capable Ethernet port.

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. 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

aggregate-policer-name	Name of the aggregate policer referenced by the **police aggregate** policy-map class configuration command.
rate-bps	Specify average traffic rate in bits per second (bps). The range is 8000 to 1000000000.
burst-byte	Specify the normal burst size in bytes. The range is 8000 to 2000000.
exceed-action drop	When the specified rate is exceeded, specify that the switch drop the packet.
exceed-action policed-dscp-transmit	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

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(25)SE	The ranges for *rate-bps* and *burst-bps* was changed.

Usage Guidelines

Define an aggregate policer if the policer is shared with multiple classes.

Policers in one port cannot be shared with other policers in another port; traffic from two different ports cannot be aggregated for policing purposes.

You cannot attach an aggregate policer to the ingress or egress of the same port.

Although the command-line help strings show a large range of values, the *rate-bps* option cannot exceed the configured port speed. If you enter a larger value, the switch rejects the policy map when you attach it to an interface.

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps or interfaces.

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.

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 apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 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

Command	Description
police aggregate	Creates a policer that is shared by different classes.
show mls qos aggregate-policer	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 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**}

Syntax Description

default-cos	Assign a default CoS value to a port. If the port is CoS trusted and packets are untagged, the default CoS value becomes a CoS value used to select one output queue to index into the CoS-to-Differentiated Services Code Point (DSCP) map. The CoS range is 0 to 7.
override	Override the CoS of the incoming packets, and apply the default CoS value on the port to all incoming packets.

Defaults

The default CoS value for a port is 0.

CoS override is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You can use the default value to assign a CoS and DSCP value to all packets entering a port if the port has been configured with the **override** 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.

Examples

This example shows how to configure the default port CoS to 4:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos cos 4
```

This example shows how to assign all the packets entering a port to the default port CoS value of 4:

```
Switch(config)# interface gigabitethernet0/1
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
show mls qos interface	Displays quality of service (QoS) information.

mls qos cos policy-map

Use the **mls qos cos policy-map** global configuration command to set the class of service (CoS) value of a port in a policy map. Use the **no** form of this command to return to the default setting.

mls qos cos policy-map

no mls qos cos policy-map

Syntax Description

This command has no arguments or keywords.

Defaults

The CoS value is not set in a policy map.

Command Modes

Global configuration

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

When using the **mls qos cos policy-map** global configuration command, you can specify the CoS value in a policy map that includes the **trust dscp** policy-map configuration command.

If you do not use the **mls qos cos policy-map** command but use the **set cos** *new-cos* policy-map class configuration command, the switch ignores the action defined by the **set cos** command in the policy map. If this policy map also has an action defined by the **trust dscp** policy-map class configuration command, the switch uses the Differentiated Services Code Point (DSCP)-to-CoS map to define the CoS value of a port.

Examples

This example shows how to define the CoS value in a policy map. When traffic matches the class map *class1*, the CoS value for traffic is set to 3, and the DSCP value does change.

```
Switch(config)# mls qos cos policy-map
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

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

Related Commands

Command	Description
class	Defines a traffic classification on which a policy acts.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces and enters policy-map configuration mode.
set	Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in the packet.
show policy-map	Displays quality of service (QoS) policy maps.
trust	Defines a trust state for traffic classified by the **class** policy-map configuration or the **class-map** global configuration command.

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 DSCP-to-DSCP-mutation map to the default settings (no DSCP mutation).

mls qos dscp-mutation *dscp-mutation-name*

no mls qos dscp-mutation *dscp-mutation-name*

Syntax Description

dscp-mutation-name	Name of the DSCP-to-DSCP-mutation map, which was previously defined with the **mls qos map dscp-mutation** global configuration command.

Defaults

The default DSCP-to-DSCP-mutation map is a null map, which maps incoming DSCPs to the same DSCP values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You apply the DSCP-to-DSCP-mutation map to a port at the boundary of a quality of service (QoS) administrative domain. If two QoS domains have different DSCP definitions between them, you use the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition of another domain. You apply the map only to ingress and to DSCP-trusted ports. Applying this map to a port causes IP packets to be rewritten with newly mapped DSCP values at the ingress 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.

You can have multiple DSCP-to-DSCP-mutation maps and apply them to different Gigabit-capable Ethernet ports. However, on 10/100 Ethernet ports, you can attach only one DSCP-to-DSCP-mutation map to a group of twelve ports. For example, Fast Ethernet ports 0/1 to 0/12 are a group, Fast Ethernet ports 0/13 to 0/24 are a group, Gigabit Ethernet port 0/1 is a group, and Gigabit Ethernet port 0/2 is a group. When applying a mutation map to any port in a group, all ports in the same group are automatically configured with the same map.

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 gigabitethernet0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation dscpmutation1
```

This example shows 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.

Related Commands

Command	Description
mls qos map dscp-mutation	Defines the DSCP-to-DSCP-mutation map.
mls qos trust	Configures the port trust state.
show mls qos maps	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 DSCP-to-switch-priority 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* | **dscp-switch-priority** *dscp-list* **to** *switch-priority* | **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* | **dscp-switch-priority** | **ip-prec-dscp** | **policed-dscp**}

Syntax Description

cos-dscp *dscp1...dscp8*	Define the CoS-to-DSCP map. For *dscp1...dscp8*, 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.
dscp-cos *dscp-list* **to** *cos*	Define the DSCP-to-CoS map. For *dscp-list*, enter up to eight DSCP values, with each value separated by a space. The range is 0 to 63. Then enter the **to** keyword. For *cos*, enter the CoS value to which the DSCP values correspond. The range is 0 to 7.
dscp-mutation *dscp-mutation-name in-dscp* **to** *out-dscp*	Define the DSCP-to-DSCP-mutation map. For *dscp-mutation-name*, enter the mutation map name. For *in-dscp*, enter up to eight DSCP values, with each value separated by a space. Then enter the **to** keyword. For *out-dscp*, enter a single DSCP value. The range is 0 to 63.
dscp-switch-priority *dscp-list* **to** *switch-priority*	Define the DSCP-to-switch-priority map. This map generates the priority of a request to the switch fabric when using a priority-aware switch fabric. For *dscp-list*, enter up to eight DSCP values, with each value separated by a space. The range is 0 to 63. Then enter the **to** keyword. For *switch-priority*, the range is 0 to 3.
ip-prec-dscp *dscp1...dscp8*	Define the IP-precedence-to-DSCP map. For *dscp1...dscp8*, 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.
policed-dscp *dscp-list* **to** *mark-down-dscp*	Define the policed-DSCP map. For *dscp-list*, enter up to eight DSCP values, with each value separated by a space. Then enter the **to** keyword. For *mark-down-dscp*, enter the corresponding policed (marked down) DSCP value. The range is 0 to 63.

Defaults

Table 2-7 shows the default CoS-to-DSCP map:

Table 2-7 Default CoS-to-DSCP Map

CoS Value	DSCP Value
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Table 2-8 shows the default DSCP-to-CoS map:

Table 2-8 Default DSCP-to-CoS Map

DSCP Value	CoS Value
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 2-9 shows the default DSCP-to-switch priority map:

Table 2-9 Default DSCP-to-Switch Priority

DSCP Value	Switch Priority
0–15	0
16–31	1
32–47	2
48–63	3

Table 2-10 shows the default IP-precedence-to-DSCP map:

Table 2-10 Default IP-Precedence-to-DSCP Map

IP Precedence Value	DSCP Value
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

Release	Modification
12.1(4)EA1	This command was introduced.

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. You can have multiple DSCP-to-DSCP-mutation maps, and apply them to different Gigabit-capable Ethernet ports. Because a group of twelve 10/100 Ethernet ports (Fast Ethernet 0/1 to 0/12, 0/13 to 0/24, and so forth) shares a single DSCP-to-DSCP-mutation map, only one map can be attached to each 10/100 group.

Examples

This example shows how to define the IP-precedence-to-DSCP map and 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.

Related Commands

Command	Description
mls qos dscp-mutation	Applies a DSCP-to-DSCP-mutation map to a DSCP-trusted port.
show mls qos maps	Displays quality of service (QoS) mapping information.

mls qos min-reserve

Use the **mls qos min-reserve** global configuration command to configure the size of the minimum-reserve levels (segments) on all 10/100 Ethernet ports. Use the **no** form of this command to return to the default setting.

mls qos min-reserve *min-reserve-level min-reserve-buffersize*

no mls qos min-reserve *min-reserve-level*

Syntax Description

min-reserve-level	Minimum-reserve level number. The range is 1 to 8.
min-reserve-buffersize	Actual minimum-reserve buffer size. The range is 10 to 170 packets.

Defaults

The buffer size for all eight minimum-reserve levels is 100 packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

When you enter this command, the switch is in a *halt* mode and drops packets for a short period.

Use the **wrr-queue min-reserve** interface configuration command to assign one of these minimum-reserve levels to an egress queue. The minimum-reserve level configuration is meaningless until it is assigned to a particular queue.

Examples

This example shows how to configure minimum-reserve level 5 to 20 packets on all 10/100 Ethernet ports:

```
Switch(config)# mls qos min-reserve 5 20
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays quality of service (QoS) information.
wrr-queue min-reserve	Assigns a minimum-reserve level to an egress queue on a 10/100 Ethernet port.

mls qos monitor

Use the **mls qos monitor** interface configuration command to define up to eight Differentiated Services Code Point (DSCP) values per command for which byte or packet statistics are gathered by hardware. Use the **no** form of this command to return to the default setting.

mls qos monitor {**bytes** | **dscp** *dscp1 ... dscp8* | **packets**}

no mls qos monitor {**bytes** | **dscp** *dscp1 ... dscp8* | **packets**}

Syntax Description

bytes	Gather statistics in bytes.
dscp *dscp1 ... dscp8*	DSCP values to be monitored. Enter up to eight values per command, with each value separated by a space. The range is 0 to 63.
packets	Gather statistics in packets.

Defaults

Statistics are not gathered for any DSCP.

If no keyword is specified when the command is entered, byte statistics are gathered.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If you want to monitor more than eight DSCP values, you must enter this command again and specify another set of DSCP values. Use this command when you want to find out how many packets are policed and dropped by the quality of service (QoS) process in hardware.

Examples

This example shows how to monitor DSCP values 10 to 20. Note that up to eight values can be entered per command.

```
Switch(config-if)# mls qos monitor dscp 10 11 12 13 14 15 16 17
Switch(config-if)# mls qos monitor dscp 18 19 20
Switch(config-if)# end
Switch# show mls qos interface statistics
```

This example shows how to gather packet statistics for DSCPs 10 to 13:

```
Switch(config-if)# mls qos monitor dscp 10 11 12 13
Switch(config-if)# mls qos monitor packets
```

You can see the results of monitoring activity by entering the **show mls qos interface statistics** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays all the DSCPs for which statistics are maintained and the corresponding ingress and egress statistics, including the number of bytes dropped, when the **statistics** keyword is appended.

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 Differentiated Services Code Point (DSCP), class of service (CoS), or IP-precedence packet field. Use the **no** form of this command to return a port to its untrusted state.

mls qos trust [**cos** [**pass-through dscp**] | **device cisco-phone** | **dscp** [**pass-through cos**] | **ip-precedence**]

no mls qos trust [**cos** [**pass-through**] | **device** | **dscp** [**pass-through**] | **ip-precedence**]

Syntax Description

cos	(Optional) Classify ingress packets with packet CoS values. For untagged packets, use the port default CoS value.
cos pass-through dscp	(Optional) Classify ingress packets by trusting the CoS value and by sending packets without modifying the DSCP value (pass-through mode).
device cisco-phone	(Optional) Classify ingress packets by trusting the CoS or DSCP value sent from the Cisco IP Phone (trusted boundary), depending on the trust setting.
dscp	(Optional) Classify ingress packets with packet DSCP values (most significant 6 bits of 8-bit service-type field). For non-IP packets, the packet CoS is used if the packet is tagged. The default port CoS value is used if the packet is untagged.
dscp pass-through cos	(Optional) Classify ingress packets by trusting the DSCP value and by sending packets without modifying the CoS value (pass-through mode).
ip-precedence	(Optional) Classify ingress packets with IP-precedence values (most significant 3 bits of 8-bit service-type field). For non-IP packets, the packet CoS is used if the packet is tagged. The port default CoS value is used if the packet is untagged.

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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **device cisco-phone**, **pass-through cos**, and **pass-through dscp** keywords were added.
12.1(20)EA2	The usage guidelines were revised to describe how the switch sets the trust state when a Cisco IP Phone is connected to a switch or routed port.

Usage Guidelines

Packets entering a quality of service (QoS) domain are classified at the edge of the QoS 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 derives 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 the CP-to-CoS map) unless the **pass-through cos** keyword is specified.

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to the CoS-to-DSCP map) if the packet is an IP packet (unless the **pass-through dscp** keyword is specified).

If you configure the **mls qos trust** [**cos pass-through dscp** | **dscp pass-through cos**] interface configuration command and then configure the **mls qos trust** [**cos** | **dscp**] interface configuration command, pass-through mode is disabled.

If you configure an interface for DSCP pass-through mode by using the **mls qos trust cos pass-through dscp** interface configuration command and apply the DSCP-to-DSCP mutation map to the same interface, the DSCP value changes according to the mutation map.

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 (sets the trust state to not trusted) 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.

A classification that uses a port trust state (for example, **mls qos trust** [**cos** | **dscp** | **ip-precedence**] and classification that uses a policy map (for example, **service-policy input** *policy-map-name*) are mutually exclusive. The last setting configured overwrites the previous configuration.

Examples

This example shows how to configure a port as an IP-precedence trusted port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust ip-precedence
```

This example shows how to specify that the Cisco IP Phone is a trusted device:

```
Switch(config)# interface fastethernet0/1
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

Command	Description
mls qos cos	Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port.
mls qos dscp-mutation	Applies a DSCP-to DSCP-mutation map to a DSCP-trusted port.
mls qos map	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.
show mls qos interface	Displays QoS information.

monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) session, 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 source 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.

monitor session *session_number* {**destination** {**interface** *interface-id* [**encapsulation** {**dot1q** [**ingress vlan** *vlan-id*] | **ISL** [**ingress**]} [**ingress vlan** *vlan-id*] | **remote vlan** *vlan-id* **reflector-port** *interface-id*} | **filter vlan** *vlan-id* [, | -] | {**source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**] | **remote vlan** *vlan-id* | **vlan** *vlan-id* [, | -] **rx**}}

no monitor session *session_number* {**destination** {**interface** *interface-id* [**encapsulation** {**dot1q** [**ingress vlan** *vlan-id*] | **ISL** [**ingress**]} [**ingress vlan** *vlan-id*] | **remote vlan** *vlan-id* **reflector-port** *interface-id*} | **filter vlan** *vlan-id* [, | -] | {**source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**] | **remote vlan** *vlan-id* | **vlan** *vlan-id* [, | -] **rx**}}

no monitor session {*session_number* | **all** | **local** | **remote**}

Syntax Description

session_number	Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 2.
destination interface *interface-id*	Specify the destination interface for a local SPAN session. Valid interfaces are physical ports.
encapsulation	(Optional) Specify the encapsulation header for outgoing packets through a destination port. If encapsulation type is not specified, packets are sent in native form. To reconfigure a destination port in native form, enter the command without the **encapsulation** keyword.
dot1q	(Optional) Specify the encapsulation type as IEEE 802.1Q.
isl	(Optional) Specify the encapsulation type as ISL.
ingress vlan *vlan-id*	(Optional) Specify whether forwarding is enabled for ingress traffic on the destination port. • For native (untagged) and dot1q encapsulation, specify **ingress vlan** *vlan-id* to enable ingress forwarding with *vlan id* as the native VLAN. *Vlan-id* is also used as the native VLAN for transmitted packets. • Specify **ingress** to enable ingress forwarding when using ISL encapsulation.
destination remote vlan *vlan-id*	Specify the destination remote VLAN for an RSPAN source session.
reflector-port *interface-id*	Specify the reflector port used for a source RSPAN session.
filter vlan *vlan-id*	Specify a list of VLANs as filters on trunk source ports. The range is 1 to 4094.
source interface *interface-id*	Specify the SPAN source interface type, slot, and port number. Valid interfaces include physical ports and port channels.

,	(Optional) Specify a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space after the comma. **Note** For **source interface**, you can configure the first port to monitor egress traffic; other ports will be ingress only if a range or list is specified.
-	(Optional) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen. **Note** For **source interface**, you can configure the first port to monitor egress traffic; other ports will be ingress only if a range or list is specified.
both, rx, tx	(Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic. Transmitted (**tx**) traffic can be monitored on only one source port.
source remote vlan *vlan-id*	Specify the source RSPAN VLAN for an RSPAN destination session.
source vlan *vlan-id* **rx**	Specify the SPAN or RSPAN source interface as a VLAN ID. The range is 1 to 4094. VLANs cannot be egress monitored. Direction (**rx**) must be specified.
all, **local**, **remote**	Specify **all**, **local**, or **remote** to clear a SPAN or RSPAN session.

Defaults

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

All VLANs are monitored on a trunk interface that is used as a source port.

If encapsulation type is not specified on a destination port, packets are sent in native form with no encapsulation.

Ingress forwarding is disabled on destination ports.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA1	This command was introduced.
12.1(11)EA1	These RSPAN keywords were added: **destination remote vlan reflector-port**, **source remote vlan**, **all**, **local**, **remote**.
12.1(12c)EA1	The **ingress vlan** keyword was added.

Usage Guidelines

Traffic that enters or leaves source ports or enters 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 maximum of two SPAN or RSPAN sessions. You can divide the two sessions between SPAN, RSPAN source, and RSPAN destination sessions. Each session can have only one destination port and only one transmitting source port. You can, however, have multiple receiving source ports and VLANs.

You can monitor only received traffic on a VLAN; you cannot monitor transmitted traffic.

You can monitor traffic on a single port or VLAN or on a series or range of ports (ingress traffic only) 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 or reflector ports. A physical port that is a member of an EtherChannel group can be used as a source or destination port. It cannot participate in the EtherChannel group while it is configured for SPAN or RSPAN.

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

A port used as a destination port cannot be a SPAN or RSPAN source or reflector port, 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 will return an error message.) You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

If ingress forwarding is enabled, you can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) Sensor Appliance to a destination port, the IDS device can send TCP Reset packets to close down the TCP session of a suspected attacker.

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.

VLAN-based SPAN (VSPAN) refers to analyzing network traffic in a 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.

Trunk VLAN filter 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 the trunk source port to only the specified VLANs.

Examples

This example shows how to create SPAN session 1 to monitor both sent and received traffic on a source interface and on a destination interface:

```
Switch(config)# monitor session 1 source interface fastEthernet0/1 both
Switch(config)# monitor session 1 destination interface fastEthernet0/8
```

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

```
Switch(config)# no monitor session 2 destination fastEthernet0/4
```

This example shows how to limit SPAN traffic only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 304
```

This example shows how to configure RSPAN session 1 to monitor multiple source interfaces and a VLAN and to configure the destination RSPAN VLAN and the reflector-port:

```
Switch(config)# monitor session 1 source interface fastethernet0/10 tx
Switch(config)# monitor session 1 source interface fastethernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 source vlan 5 rx
Switch(config)# monitor session 1 destination remote vlan 901 reflector-port
fastethernet 0/1
Switch(config)# end
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support IEEE 802.1Q encapsulation:

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 ingress vlan 5
```

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:

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation
dot1q ingress vlan 5
```

This example shows how to disable ingress traffic forwarding on the destination port:

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation
dot1q
```

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

Related Commands

Command	Description
remote-span	Configures an RSPAN VLAN in vlan configuration mode.
show monitor	Displays SPAN and RSPAN session information.

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

group *ip-address*	Statically configure an MVR group IP multicast address on the switch. Use the **no** form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses.
count	(Optional) Configure multiple contiguous MVR group addresses. The range is 1 to 256; the default is 1.
mode	(Optional) Specify the MVR mode of operation. The default is compatible mode.
compatible	Set MVR mode to provide compatibility with Catalyst 2900 XL and 3500 XL switches. This mode does not allow dynamic membership joins on source ports.
dynamic	Set MVR mode to allow dynamic MVR membership on source ports.
querytime *value*	(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 **no** form of the command to return to the default setting.
vlan *vlan-id*	(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.

Command Modes Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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.

Note The **mvr group** command prevents adding IP multicast addresses that cause address aliasing between MVR multicast groups or with the reserved IP multicast addresses (in the range 224.0.0.xx). Each IP multicast address translates to a multicast 48-bit MAC address. If the IP address being configured translates (aliases) to the same 48-bit MAC address as a previously configured IP multicast address or the reserved MAC multicast addresses, the command fails.

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.

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

Examples This example shows how to enable MVR:

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

This example shows how to disable MVR:

```
Switch(config)# no 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 command fails because of address aliasing:

```
Switch(config)# mvr group 230.1.23.4

Cannot add this IP address - aliases with previously configured IP address 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
```

This example shows how to delete the previously configured ten IP multicast addresses:

```
Switch(config)# no mvr group 228.1.23.1 10
```

This example shows how to delete all previously configured IP multicast addresses:

```
Switch(config)# no mvr group
```

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 return the maximum query response time to the default setting of one-half second:

```
Switch(config)# no mvr querytime
```

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

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

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

Related Commands

Command	Description
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	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.
show mvr members	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*]}

Syntax Description

immediate	(Optional) Enable the Immediate Leave feature of MVR on a port. Use the **no mvr immediate** command to disable the feature.
type	(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 **no mvr type** command resets the port as neither a source or a receiver port.
receiver	Configure the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN.
source	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.
vlan *vlan-id* **group** *ip-address*	(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. If the entered VLAN is not the multicast VLAN, an error message is reported. The **no mvr vlan group** command removes a port on a VLAN from membership in an IP multicast address group. With the **no** form, the IP address is optional; when no IP address is entered, the specified port is removed from membership in all configured multicast groups.

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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr type receiver
```

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

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr type source
```

This example shows how to remove a port as an MVR port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if))# no mvr
```

This example shows how to display configured receiver ports and source ports.

```
Switch# show mvr interface
Port    Type            Status          Immediate Leave
----    ----            -------         ---------------
Gi0/1   SOURCE          ACTIVE/UP       DISABLED
Gi0/2   RECEIVER        ACTIVE/DOWN     DISABLED
Gi0/5   RECEIVER        ACTIVE/UP       ENABLED
```

This example shows how to enable immediate leave on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr immediate
```

This example shows how to disable immediate leave on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr immediate
```

To display the MVR status and whether or not immediate leave is enabled on an interface, use the **show mvr** privileged EXEC command for the interface, as in this example:

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This example shows how to add a port 2 on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

This example shows how to remove this port from membership:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr vlan5 group 228.1.23.4
```

This example shows how to remove this port from all IP multicast groups:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no mvr vlan5 group
```

This example shows the result if a port is not a receiver port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan 1 group 230.1.23.4
Interface Gi0/2 not configured as a receiver interface
```

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

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
show mvr	Displays MVR global parameters or port parameters.
show mvr interface	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.
show mvr members	Displays all receiver ports that are members of an MVR multicast group.

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

Syntax Description

aggregation-port	Specify address learning on the logical port-channel. The switch sends packets to the source by using any of the interfaces in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
physical-port	Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source by using the same interface 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

Release	Modification
12.1(4)EA1	This command was introduced.

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 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 Catalyst 3550 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
pagp port-priority	Selects an interface over which all traffic through the EtherChannel is sent.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

pagp port-priority

Use the **pagp port-priority** interface configuration command to select an interface over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. If all unused interfaces in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected interface and link fail. Use the **no** form of this command to return to the default setting.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	A priority number ranging from 0 to 255.

Defaults

The default value is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

Note The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the 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 Catalyst 3550 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 port priority to 200:

```
Switch(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Related Commands

Command	Description
pagp learn-method	Provides the ability to learn the source address of incoming packets.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

permit

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, nor is matching on any SNAP-encapsulated packet with a non-zero Organizational Unique Identifier (OUI).

Syntax Description

any	Keyword to specify to deny any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	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.
host *dst-MAC-addr* | *dst-MAC-addr mask*	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.
type mask	(Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. • *type* is from 0 to 65535, typically specified in hexadecimal. • *mask* is a mask of *don't care* bits applied to the Ethertype before testing for a match.
aarp	(Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Select EtherType DEC-Amber.
cos *cos*	(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 **cos** option is configured.
dec-spanning	(Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Select EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Select EtherType DEC-Diagnostic.
dsm	(Optional) Select EtherType DEC-DSM.
etype-6000	(Optional) Select EtherType 0x6000.
etype-8042	(Optional) Select EtherType 0x8042.

lat	(Optional) Select EtherType DEC-LAT.
lavc-sca	(Optional) Select EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Use the LSAP number (0 to 65535) of a packet with IEEE 802.2 encapsulation to identify the protocol of the packet. The *mask* is a mask of *don't care* bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Select EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Select EtherType DEC-MOP Dump.
msdos	(Optional) Select EtherType DEC-MSDOS.
mumps	(Optional) Select EtherType DEC-MUMPS.
netbios	(Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Select EtherType VINES IP.
xns-idp	(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 2-11.

Table 2-11 IPX Filtering Criteria

IPX Encapsulation Type		
Cisco IOS Name	**Novell Name**	**Filter Criterion**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet IEEE 802.2	LSAP 0xE0E0
novell-ether	Ethernet IEEE 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

Release	Modification
12.1(4)EA1	This command was introduced.

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.

Note 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 name 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 name 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

Command	Description
deny	Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

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*}]} [l**og**]

Syntax Description

request	(Optional) Requests a match for the ARP request. When **request** is not specified, matching is performed against all ARP packets.
ip	Specify the sender IP address.
any	Accept any IP or MAC address.
host *sender-ip*	Accept the specified sender IP address.
sender-ip sender-ip-mask	Accept the specified range of sender IP addresses.
mac	Specify the sender MAC address.
host *sender-mac*	Accept the specified sender MAC address.
sender-mac sender-mac-mask	Accept the specified range of sender MAC addresses.
response ip	Define the IP address values for the ARP responses.
host *target-ip*	(Optional) Accept the specified target IP address.
target-ip target-ip-mask	(Optional) Accept the specified range of target IP addresses.
mac	Specify the MAC address values for the ARP responses.
host *target-mac*	(Optional) Accept the specified target MAC address.
target-mac target-mac-mask	(Optional) Accept the specified range of target MAC addresses.
log	(Optional) Log a packet when it matches the ACE. Matches are logged if you also configure the **matchlog** keyword in the **ip arp inspection vlan logging** global configuration command.

Defaults

There are no default settings.

Command Modes

ARP access-list configuration

Command History

Release	Modification
12.2(25)SEA	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
arp access-list	Defines an ARP ACL.
deny (ARP access-list configuration)	Denies an ARP packet based on matches against the DHCP bindings.
ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
show arp access-list	Displays detailed information about ARP access lists.

police

Use the **police** policy-map class configuration command to define a policer for classified traffic. 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

rate-bps	Specify average traffic rate in bits per second (bps). The range is 8000 to 1000000000.
burst-byte	Specify the normal burst size in bytes. The range is 8000 to 2000000.
exceed-action drop	(Optional) When the specified rate is exceeded, specify that the switch drop the packet.
exceed-action policed-dscp-transmit	(Optional) 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 policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(25)SE	The ranges for *rate-bps* and *burst-bps* was changed.

Usage Guidelines

You can configure up to 128 policers on ingress Gigabit-capable Ethernet ports.

You can configure up to eight policers on ingress 10/100 Ethernet ports.

You can configure up to eight policers on egress ports.

Although the command-line help strings show a large range of values, the *rate-bps* option cannot exceed the configured port speed. If you enter a larger value, the switch rejects the policy map when you attach it to an interface.

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.

Examples

This example shows how to configure a policer that drops packets if traffic exceeds a 1-Mbps average rate and a 20-KB burst. 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)# set dscp 45
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 DSCPs 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

Command	Description
mls qos map policed-dscp	Applies a policed-DSCP map to a DSCP-trusted port.
show policy-map	Displays quality of service (QoS) policy maps.

police aggregate

Use the **police aggregate** policy-map class configuration command to apply an aggregate policer to multiple classes in the same policy map. Use the **no** form of this command to remove the specified policer.

police aggregate *aggregate-policer-name*

no police aggregate *aggregate-policer-name*

Syntax Description

aggregate-policer-name	Name of the aggregate policer.

Defaults

No aggregate policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You set aggregate policer parameters by using the **mls qos aggregate-policer** global configuration command.

You can configure up to 128 policers on ingress Gigabit-capable Ethernet ports.

You can configure up to eight policers on ingress 10/100 Ethernet ports.

You can configure up to eight policers on egress ports.

You apply an aggregate policer to multiple classes in the same policy map; you cannot use an aggregate policer across different policy maps or interfaces.

Policy maps that contain per-port per-VLAN classification commands cannot be applied to egress interfaces.

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 the aggregate policer parameters and apply the policer to multiple classes in a policy map:

```
Switch(config)# mls qos aggregate-policer agg_policer1 10000 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

Command	Description
mls qos aggregate-policer	Defines policer parameters, which can be shared by multiple classes within a policy map.
show mls qos aggregate-policer	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 interfaces 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*

Syntax Description

policy-map-name	Name of the policy map.

Defaults

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.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Entering the **policy-map** command enables the policy-map configuration mode. These configuration commands are available:

- **class**: defines the classification match criteria for the specified class map. For more information, see the "class" section on page 2-39.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns you to global configuration mode.
- **no**: removes a previously defined policy map.
- **rename**: renames the current policy map.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before you can configure policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. You use the **class-map** global configuration and **match** class-map configuration commands to configure the match criteria for a class. You define packet classification on a physical-port basis and on a per-port per-VLAN basis.

Only one policy map per interface per direction is supported. You can apply the same policy map to multiple interfaces and directions.

Per-port per-VLAN policing is not supported on routed ports or on virtual (logical) interfaces. It is supported only on an ingress port configured as a trunk or as a static-access port.

You cannot use the **service-policy** interface configuration command to attach policy maps that contain these elements to an egress interface:

- **set** or **trust** policy-map class configuration commands. Instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

The only match criterion in a policy map that can be attached to an egress interface is the **match ip dscp** *dscp-list* class-map configuration command.

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 DSCP to 10, and polices the traffic at an average rate of 1 Mbps and 20-KB bursts. Traffic exceeding the profile is marked down to a DSCP value obtained 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 create a policy map that contains a per-port per-VLAN classification and how to attach it to an ingress interface. A class map, called *vlan_class*, matches traffic received on VLANs 10, 20 to 30, and 40 that contains IP DSCP 9 (defined in class map *dscp_class*). If the specified average traffic rates and the burst sizes are exceeded, the switch drops the packet.

```
Switch(config)# class-map match-any dscp_class
Switch(config-cmap)# match ip dscp 9
Switch(config-cmap)# exit
Switch(config)# class-map match-all vlan_class
Switch(config-cmap)# match vlan 10 20-30 40
Switch(config-cmap)# match class-map dscp_class
Switch(config-cmap)# exit
Switch(config)# policy-map policymap2
Switch(config-pmap)# class vlan_class
Switch(config-pmap-c)# police 80000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input policymap2
```

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

Command	Description
class	Defines a traffic classification for the policy to act on.
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
police	Defines a policer for classified traffic.
set	Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in the packet.
show policy-map	Displays quality of service (QoS) policy maps.
trust	Defines a trust state for traffic classified by the **class** or the **class-map** command.

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-mac** | **src-mac**}

no port-channel load-balance

Syntax Description

dst-mac	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.
src-mac	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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

When **src-mac** is used, load distribution based on the source and destination IP address is also enabled. For all IP traffic being routed, the switch chooses a port for transmission based on the source and destination IP address. Packets between two IP hosts always use the same port for packet transmission, but packets between any other pair of hosts might use a different transmission port.

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
interface port-channel	Accesses or creates the port channel.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

power inline

Use the **power inline** interface configuration command to enable or disable the Power over Ethernet (PoE) ports on the Catalyst 3550-24PWR switch. Use the **no** form of this command to return to the default settings.

power inline {**auto** | **never**} | [**delay** {**shutdown** *seconds* **initial** *seconds*}]

no power inline

Syntax Description

auto	Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection.
never	Disable device detection and disable power to the port.
delay {**shutdown** *seconds* **initial** *seconds*}	(Optional) Power shutdown delay time. The keywords have these meanings: • **shutdown** *seconds*—Time that the switch continues to provide power to the device after linkdown. The range is 0 to 20 seconds. • **initial** *seconds*—Initial time that the power shutdown delay is in effect. The range is 0 to 300 seconds.

Defaults

The default is **auto**.

No delay time is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.
12.1(19)EA1	The **delay shutdown** *seconds* **initial** *seconds* keywords were added.

Usage Guidelines

This command is supported only on PoE-capable ports. PoE ports were previously referred to as inline power ports in earlier versions of the command reference.

When you configure a port by using the **power inline auto** interface configuration command, the port autonegotiates by using the configured speed and duplex settings to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements are 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 command disables the detection and power for the PoE-capable port, and 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.

Use the **power inline delay shutdown** *seconds* **initial** *seconds* command for certain IEEE-compliant powered devices that require multiple reloads during initialization. With this setting, the switch continues to provide power during initialization. Without the **delay shutdown** keywords, the switch immediately removes power when linkdown occurs on the connected device.

When the switch is connected to a Cisco powered device, the **delay shutdown** keywords are not needed. Although you can configure a delay shutdown time, it does not take any action on a connected Cisco device.

Caution To avoid product damage, you should not connect any device that is not IEEE-compliant during the delay shutdown time interval. When the **delay shutdown** keywords are active on a port, the port remains powered after unplugging the IEEE-compliant powered device for the configured time interval.

The initial time period begins when the IEEE-compliant powered device is detected by the switch. If linkdown occurs on the connected device during the initial time period, the shutdown time determines how long the switch continues to provide power to the device.

Use the **no power inline delay shutdown** *seconds* **initial** *seconds* interface configuration command to return to the default setting.

Examples

This example shows how to disable PoE detection and to not power a PoE port:

```
Switch(config-if)# power inline never
```

This example shows how to enable PoE detection and to automatically power a PoE port:

```
Switch(config-if)# power inline auto
```

This example shows how to configure a shutdown time delay for an IEEE powered device:

```
Switch(config-if)# power inline delay shutdown 20 initial 90
```

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

Related Commands

Command	Description
show interfaces transceiver properties	Displays the inline power status for a PoE port.
show power inline	Displays the power 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 Gigabit-capable or a 10/100 Ethernet interface. Use the **no** form of this command to return to the default setting.

priority-queue out

no priority-queue out

Syntax Description

out	Enable the egress expedite queue.

Defaults

The egress expedite queue is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

When you configure the **priority-queue out** command, the weighted round robin (WRR) weight ratios are affected because there is one fewer queue participating in WRR. This means that *weight4* in the **wrr-queue bandwidth** 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.

Examples

This example shows how to enable the egress expedite queue:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# priority-queue out
```

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

Related Commands

Command	Description
show mls qos interface queueing	Displays the queueing strategy (WRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.

rcommand

Use the **rcommand** user EXEC command to start a Telnet session and to execute commands on a member switch from the command switch. To end the session, enter the **exit** command.

rcommand {*n* | **commander** | **mac-address** *hw-addr*}

Syntax Description

n	Provide the number that identifies a cluster member. The range is 0 to 15.
commander	Provide access to the command switch from a member switch.
mac-address *hw-addr*	MAC address of the member switch.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If the switch is the command switch but the member switch *n* does not exist, an error message appears. To obtain the switch number, enter the **show cluster members** privileged EXEC command on the command switch.

You can use this command to access a member switch from the command-switch prompt or to access a command switch from the member-switch prompt.

For Catalyst 2900 XL, 3500 XL, 2950, and 3550 switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the command switch. For example, if you execute this command at user level on the cluster command switch, the member switch is accessed at user level. If you use this command on the 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 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 command switch is at privilege level 15. If the command switch is at privilege level 1, you are prompted for the password before being able to access the menu console. Command switch privilege levels map to the member switches running standard edition software as follows:

- If the command switch privilege level is from 1 to 14, the member switch is accessed at privilege level 1.
- If the command switch privilege level is 15, the 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 command switch have access-class configurations.

You are not prompted for a password because the member switches inherited the password of the 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
show cluster members	Displays information about the cluster members.

remote-span

Use the **remote-span** VLAN configuration command to add the Remote Switched Port Analyzer (RSPAN) feature to a VLAN. Use the **no** form of this command to remove the RSPAN feature 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

Command History

Release	Modification
12.1(11)EA1	This command was introduced.

Usage Guidelines

When a VLAN is converted from a normal VLAN to an RSPAN VLAN (or the reverse), the VLAN is first deleted and is then recreated with the new configuration. If VTP is enabled, the RSPAN feature is propagated by VLAN Trunking Protocol (VTP) for VLAN-IDs that are lower than 1024.

Before you configure the RSPAN **remote-span** feature, use the **vlan** (global configuration) command to create the VLAN.

Examples

This example shows how to configure 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** user EXEC command.

Related Commands

Command	Description
monitor session	Enables Switched Port Analyzer (SPAN) and RSPAN monitoring on a port and configures a port as a source or destination port.
vlan (global configuration)	Changes to config-vlan mode where you can configure VLANs 1 to 4094; do not enter leading zeros.

rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include utilization 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*]

Syntax Description

index	Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
owner *name*	(Optional) Owner of the RMON collection.

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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* on an interface:

```
Switch(config)# interface gigabitethernet0/1
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
show rmon statistics	Displays RMON statistics. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > System Management Commands > RMON Commands**.

sdm prefer

Use the **sdm prefer** global configuration command to configure the template used in Switch Database Management (SDM) resource allocation. You use a template to allocate system memory to best support the features being used in your application. Use a template to approximate the maximum number of unicast MAC addresses, Internet Group Management Protocol (IGMP) groups, quality of service (QoS) access control entries (ACEs), security ACEs, unicast routes, multicast routes, subnet VLANs (routed interfaces), and Layer 2 VLANs that can be configured on the switch. Use the **no** form of this command to return to the default template.

sdm prefer {**access** [**extended-match**] | **extended-match** | **routing** [**extended-match**] | **vlan**}

no sdm prefer

Syntax Description

access	Provide maximum system utilization for multicast traffic, QoS classification ACEs, and security ACEs. You would typically use this template for an access switch at the network edge.
extended-match	Reformat routing-table memory allocation to allow 144-bit Layer 3 ternary content addressable memory (TCAM) with the default template, the access template, or the routing template. Reformatting routing table memory space reduces the number of allowed unicast routes by one half.
routing	Provide maximum system utilization for unicast routing, minimizing QoS classification ACLs and security ACLs. You would typically use this template for a router or aggregator in the middle of a network.
vlan	Provide maximum system utilization for VLANs, with routing disabled. This template maximizes system memory for use as a Layer 2 switch with no routing.

Defaults

The default template provides a balance to all features.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(6)EA1	Template values revised. Templates for Fast Ethernet switches were added.
12.1(8)EA1	Template values for Gigabit Ethernet switches were revised.
12.1(11)EA1	The **extended-match** keyword was added.

Usage Guidelines

You must reload the switch for the configuration to take effect.

The **sdm prefer vlan** command disables routing capability in the switch. Any routing configurations are rejected after the **reload**, and any previously configured routing options might be lost. Use the **sdm prefer vlan** command only on switches intended for Layer 2 switching with no routing.

Do not use the routing template if you do not have routing enabled on your switch. Entering the **sdm prefer routing** global configuration command prevents other features from using the memory allocated to unicast and multicast routing in the routing template (approximately 17 K for Fast Ethernet switches and 30 K for Gigabit Ethernet switches).

When running the Web Cache Communication Protocol (WCCP) or multiple Virtual Private Network (VPN) routing/forwarding (multi-VRF) instances in customer edge (CE) devices (multi-VRF CE), extra fields are required in the routing tables stored in TCAM. You must use the **extended-match** keyword with the default, access, or routing templates to enable the switch to support 144-bit Layer 3 TCAM when using these features. The keyword reformats the memory space allocated for routing, reducing the number of allowed unicast routes by half.

Table 2-12 lists the approximate number of each resource supported in each of the four templates for a Gigabit Ethernet switch. Table 2-13 lists the approximate number supported for a switch with mostly Fast Ethernet ports. The first six rows in the tables (unicast MAC addresses through multicast routes) represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance.

The last two rows, the total number of routed ports and SVIs and the number of Layer 2 VLANs, are guidelines used to calculate hardware resource consumption related to the other resource parameters.

The number of subnet VLANs (routed ports and SVIs) are not limited by software and can be set to a number higher than indicated in the tables. If the number of subnet VLANs configured is lower or equal to the number in the tables, the number of entries in each category (Unicast addresses, IGMP groups, and so on) for each template will be as indicated. As the number of subnet VLANs is increased, CPU utilization will typically increase. If the number of subnet VLANs is increased beyond the number indicated in the tables, the number of supported entries in each category may decrease depending on features that are enabled. For example, if PIM-DVMRP is enabled with more than 16 subnet VLANs, the number of entries for multicast routes will be in the range of 1K-5K entries for the access template.

Table 2-12 Approximate Number of Feature Resources Allowed by Each Template for Gigabit Ethernet Switches

Resource	Default Template	Access Template	Routing Template	VLAN Template
Unicast MAC addresses	6 K	2 K	6 K	12 K
IGMP groups (managed by Layer 2 multicast features such as MVR or IGMP snooping)	6 K	8 K	6 K	6 K
QoS classification ACEs	2K	2 K	1 K	2 K
Security ACEs	2 K	4 K	1 K	2 K
Unicast routes	12 K or 6 K[1]	4 K or 2 K[1]	24 K or 12 K[1]	0
Multicast routes	6 K	8 K	6 K	0
Routed interfaces (routed ports and SVIs)	16	16	16	16
Layer 2 VLANs	1 K	1 K	1 K	1 K

1. When the **extended-match** keyword is used with the indicated template. This keyword affects only the number of unicast routes allowed.

Table 2-13 Approximate Number of Feature Resources Allowed by Each Template for Fast Ethernet Switches

Resource	Default Template	Access Template	Routing Template	VLAN Template
Unicast MAC addresses	5 K	1 K	5 K	8 K
IGMP groups (managed by Layer 2 multicast features such as MVR and IGMP snooping)	1 K	2 K	1 K	1 K
QoS ACEs	1 K	1 K	512	1 K
Security ACEs	1 K	2 K	512	1 K
Unicast routes	8 K or 4K[1]	2 K or 1K[1]	16 K or 8K[1]	0
Multicast routes	1 K	2 K	1 K	0
Routed interfaces (routed ports and SVIs)	8	8	8	8
Layer 2 VLANs	1 K	1 K	1 K	1 K

1. When the **extended-match** keyword is used with the indicated template. This keyword affects only the number of unicast routes allowed.

Examples

This example shows how to configure the routing template on the switch:

```
Switch(config)# sdm prefer routing
Switch(config)# exit
Switch# reload
```

This example shows how to configure the routing template with a 144-bit routing table allocation:

```
Switch(config)# sdm prefer routing extended-match
Switch(config)# exit
Switch# reload
```

This example shows how to remove the routing template and to use the default template with the standard 72-bit routing table allocation:

```
Switch(config)# no sdm prefer routing
Switch(config)# exit
Switch# reload
```

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

Related Commands

Command	Description
show sdm prefer	Displays the current SDM template in use or displays the templates that can be used, with approximate resource allocation per feature.

service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the boot 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

Release	Modification
12.1(6)EA1a	This command was introduced.

Usage Guidelines

This command is valid only on Catalyst 3550 Fast Ethernet switches; it is not available for Gigabit Ethernet switches.

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)?
```

If the user chooses not to reset the system back to the default configuration, the normal boot process continues, as if the **Mode** button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted.

Note 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
```

This is an example of the output from the **show version** privileged EXEC command when password-recovery is disable:

```
Switch# show version
1w6d: %SYS-5-CONFIG_I: Configured from console by console
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-IPSERVICES-M), Version 12.2(25)SEB, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 14-Feb-05 06:20 by antonino
Image text-base: 0x00003000, data-base: 0x004C1864

ROM: Bootstrap program is C3550 boot loader

flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on
System image file is
"flash:c3550-ipservices-mz.122-25.SEB/c3550-ipservices-mz.122-25.SEB.bin"
cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface

48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is disabled.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

Related Commands

Command	Description
show version	Displays version information for the hardware and firmware.

service-policy

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the input or output of a particular interface. Use the **no** form of this command to remove the policy map and interface association.

service-policy {**input** *policy-map-name* | **output** *policy-map-name*}

no service-policy {**input** *policy-map-name* | **output** *policy-map-name*}

Syntax Description

input *policy-map-name*	Apply the specified policy-map to the input of an interface.
output *policy-map-name*	Apply the specified policy-map to the output of an interface.

Note Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics it gathers.

Defaults

No policy maps are attached to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Only one policy map per interface per direction is supported.

You cannot use the **service-policy** interface configuration command to attach policy maps that contain these elements to an egress interface:

- **set** or **trust** policy-map class configuration commands. Instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

The only match criterion in a policy map that can be attached to an egress interface is the **match ip dscp** *dscp-list* class-map configuration command.

A classification that uses a port trust state (for example, **mls qos trust** [**cos** | **dscp** | **ip-precedence**] and classification that uses a policy map (for example, **service-policy input** *policy-map-name*) are mutually exclusive. The last setting configured overwrites the previous configuration.

Examples

This example shows how to apply *plcmap1* to an ingress interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input plcmap1
```

This example shows how to apply *plcmap2* to an egress interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# service-policy output plcmap2
```

This example shows how to detach *plcmap2* from an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy input plcmap2
```

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

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

set

Use the **set** policy-map class configuration command to classify IP traffic by setting a class of service (CoS), Differentiated Services Code Point (DSCP), or IP-precedence value in the packet. Use the **no** form of this command to remove the traffic classification.

set {**cos** *new-cos* | **dscp** *new-dscp* | **ip precedence** *new-precedence*}

no set {**cos** *new-cos* | **dscp** *new-dscp* | **ip precedence** *new-precedence*}

Note Beginning with Cisco IOS Release 12.2(25)SE, the **set dscp** *new-dscp* command replaces the **set ip dscp** *new-dscp* command.

Syntax Description

cos *new-cos*	New CoS value assigned to the classified traffic. The range is from 0 to 7.
dscp *new-dscp*	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.
ip precedence *new-precedence*	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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(12c)EA1	The **cos** keyword was added.
12.2(25)SE	The **ip dscp** *new-dscp* keyword was changed to **dscp** *new-dscp*.

Usage Guidelines

Within the same policy map, you should not use the **set** command with the **trust** policy-map class configuration command unless you also use the **mls qos cos policy-map** global configuration command. For information about using this command, see the "mls qos cos policy-map" section on page 2-238.

You cannot use the **service-policy** interface configuration command to attach policy maps that contain these elements to an egress interface:

- **set** or **trust** policy-map class configuration commands. Instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

The only match criterion in a policy map that can be attached to an egress interface is the **match ip dscp** *dscp-list* class-map configuration command.

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 as same 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
```

This example shows how to assign a CoS value in a policy map:

```
Switch(config)# mls qos cos policy-map
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

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

Related Commands

Command	Description
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.
trust	Defines a trust state for traffic classified by the **class** policy-map configuration command or the **class-map** 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

Release	Modification
12.1(4)EA1	This command was introduced.

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 command switch in a cluster 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, return to the setup program without saving, or return to the command-line prompt without saving the configuration.

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
!
<output truncated>

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
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
show version	Displays version information for the hardware and firmware.

setup express

Use the **setup express** global configuration command to enable Express Setup mode on the switch. This is the default setting. 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

Release	Modification
12.1(14)EA1	This command was introduced.

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 mode LEDs 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 mode LEDs begin blinking green after 2 seconds.
- On a configured switch, the mode LEDs turn solid green after a total of 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 only turn solid green *or* begin blinking green if Express Setup mode is enabled on the switch.

Related Commands

Command	Description
show setup express	Displays if Express Setup mode is active on the switch.

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**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

name	(Optional) Name of the ACL.
number	(Optional) ACL number. The range is from 1 to 2699.
hardware counters	(Optional) Display global hardware ACL statistics for switched and routed packets.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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.

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

Examples

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 13
    10 permit any
Standard IP access list permit Any
    10 permit any
Extended IP access list 101
    10 permit icmp any any conversion-error
    20 permit 234 host 172.30.40.1 host 123.23.23.2
Extended IP access list 102
    10 permit esp any any
    20 permit eigrp any any tos min-monetary-cost
Extended IP access list 103
    10 permit icmp any any 40 60
Extended IP access list CMP-NAT-ACL
    10 Dynamic Cluster-NAT permit ip any any
Extended MAC access list abc2
```

```
    10 permit host 1100.bb00.00cc host 2234.0123.2345
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
Input Drops:              0 matches (0 bytes)
Output Drops:             0 matches (0 bytes)
Input Forwarded:          234781 matches (19942889 bytes)
Output Forwarded:         0 matches (0 bytes)
Input Bridge Only:        0 matches (0 bytes)
Bridge and Route in CPU: 0 matches (0 bytes)
Route in CPU:             160 matches (10344 bytes)
```

Related Commands

Command	Description
access-list	Configures a standard or extended numbered access list on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
ip access list	Configures a named IP access list on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 > IP Services Commands**.
mac access-list extended	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 TFTP protocol.

show archive status [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

begin	(Optional) Display begins with the line that matches the *expression*.
exclude	(Optional) Display excludes lines that match the *expression*.
include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SE	This command was introduced.

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 the HTTP protocol. The **show archive status** command shows the progress of the download.

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

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
archive download-sw	Downloads a new image from a TFTP server to the switch.

show auto qos

Use the **show auto qos** user EXEC command to display the quality of service (QoS) commands entered on the interfaces on which automatic QoS (auto-QoS) configuration is enabled.

show auto qos [**interface** [*interface-id*]

Syntax Description

interface [*interface-id*]	(Optional) Display auto-QoS information for the specified interface or for all interfaces. Valid interfaces include physical ports.

Command Modes

User EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.
12.1(20)EA2	The information in the command output changed, and the user guidelines were updated.

Usage Guidelines

In releases earlier than Cisco IOS Release 12.1(20)EA2, the **show auto qos** [**interface** [*interface-id*]] command output shows the initial generated auto-QoS configuration.

In Cisco IOS Release 12.1(20)EA2 or later, the **show auto qos** command output shows only the auto-QoS commands 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.

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 map cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show running-config**

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
FastEthernet0/1
auto qos voip cisco-softphone

FastEthernet0/2
auto qos voip cisco-phone

FastEthernet0/4
auto qos voip cisco-softphone
```

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 fastethernet0/2
FastEthernet0/2
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 on 10/100 Ethernet interfaces:

```
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 min-reserve 5 170
mls qos min-reserve 6 85
mls qos min-reserve 7 51
mls qos min-reserve 8 34
mls qos
!
class-map match-all AutoQoS-VoIP-RTP-Trust
  match ip dscp 46
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp 24 26
!
!
policy-map AutoQoS-Police-SoftPhone
  class AutoQoS-VoIP-RTP-Trust
    set dscp 46
    police 320000 8000 exceed-action policed-dscp-transmit
  class AutoQoS-VoIP-Control-Trust
    set dscp 24
    police 32000 8000 exceed-action policed-dscp-transmit
!
...
interface FastEthernet0/6
 switchport mode dynamic desirable
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 wrr-queue bandwidth 10 20 70 1
 wrr-queue min-reserve 1 5
 wrr-queue min-reserve 2 6
 wrr-queue min-reserve 3 7
 wrr-queue min-reserve 4 8
 wrr-queue cos-map 1 0 1
 wrr-queue cos-map 2 2 4
 wrr-queue cos-map 3 3 6 7
```

```
 wrr-queue cos-map 4 5
 priority-queue out
!
interface FastEthernet0/7
 switchport mode dynamic desirable
!
interface FastEthernet0/8
 switchport mode dynamic desirable
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 wrr-queue bandwidth 10 20 70 1
 wrr-queue min-reserve 1 5
 wrr-queue min-reserve 2 6
 wrr-queue min-reserve 3 7
 wrr-queue min-reserve 4 8
 wrr-queue cos-map 1 0 1
 wrr-queue cos-map 2 2 4
 wrr-queue cos-map 3 3 6 7
 wrr-queue cos-map 4 5
 priority-queue out
!
<output truncated>
```

These are examples 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
```

These are examples of output from the **show auto qos interface** *interface-id* command when auto-QoS is disabled on an interface:

```
Switch> show auto qos interface fastethernet0/1
AutoQoS is disabled
```

Related Commands

Command	Description
auto qos voip	Automatically configures QoS for VoIP within a QoS domain.

show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

show boot [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The Private Config file field description was added.

Usage Guidelines

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

Note Only the Cisco IOS software can read and write a copy of the private configuration file. You cannot read, write, delete, or display a copy of this file.

Examples

This is an example of output from the **show boot** command. Table 2-14 describes each field in the display.

```
Switch# show boot
BOOT path-list:
flash:c3550-ipservices-mz-122-25.SEB/c3550-ipservices-mz-122-25.SEB.bin
Config file:         flash:config.text
Private Config file: flash:private-config.text
Enable Break:        no
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
      buffer size:   32768
```

Table 2-14 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. 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 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 private configuration. **Note** Only the Cisco IOS software can read and write a copy of the private configuration file. You cannot read, write, delete, or display a copy of this file.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
NVRAM/Config file buffer size	Displays the buffer size that Cisco IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation.

Related Commands

Command	Description
boot buffersize	Specifies the size of the file system-simulated NVRAM in flash memory.
boot config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
boot enable-break	Enables interrupting the automatic boot process.
boot manual	Enables manually booting the switch during the next boot cycle.
boot private-config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
boot system	Specifies the Cisco IOS image to load during the next boot cycle.

show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

show class-map [*class-map-name*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

class-map-name	(Optional) Display the contents of the specified class map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show class-map** command:

```
Switch> show class-map
 Class Map match-any dscp_class
   Match ip dscp 9
Class Map match-all vlan_class
  Match vlan 10 20-30 40
  Match class-map dscp_class
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match (class-map configuration)	Defines the match criteria to classify traffic.

show cluster

Use the **show cluster** user EXEC command to display the cluster status and a summary of the cluster to which the switch belongs. This command can be entered on command and member switches.

show cluster [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If the switch is not a command switch or a member switch, the command displays an empty line at the prompt.

On a member switch, this command displays the identity of the command switch, the switch member number, and the state of its connectivity with the command switch.

On a 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.

If you enter this command on a switch that is not a cluster member, the error message `Not a management cluster member` appears.

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

Examples

This is an example of output when the **show cluster** command is entered on the active 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 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 member switch that is configured as the standby command switch:

```
Switch> 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 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 member switch that has lost connectivity with the 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

Command	Description
cluster enable	Enables a command-capable switch as the cluster command switch, assigns a cluster name, and optionally assigns a member number to it.
show cluster candidates	Displays a list of candidate switches.
show cluster members	Displays information about the cluster members.

show cluster candidates

Use the **show cluster candidates** privileged EXEC command on the command switch to display a list of candidate switches.

show cluster candidates [**detail** | **mac-address** *H.H.H.*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	(Optional) Display detailed information for all candidates.
mac-address *H.H.H.*	(Optional) MAC address of the cluster candidate.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Enter this command only on a command switch.

If the switch is not a command switch, the command returns 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 command switch.

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

Examples

This is an example of output from the **show 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-C3550-12T     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   0  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 member switch directly connected to the 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-C3512-XL
        Upstream MAC address:   00d0.796d.2f00 (Cluster Member 0)
        Local port:             Fa0/3   FEC number:
        Upstream port:          Fa0/13  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 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
        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

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster members	Displays information about the cluster members.

show cluster members

Use the **show cluster members** privileged EXEC command on the command switch to display information about the cluster members.

show cluster members [*n* | **detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

n	(Optional) Number that identifies a cluster member. The range is from 0 to 15.
detail	(Optional) Display detailed information for all cluster members.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You should enter this command only on a command switch.

If the cluster has no members, this command displays an empty line at the prompt.

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

Examples

This is an example of output from the **show 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-C3550-12T
        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
```

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-C3550-12T
        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
        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-C3550-12T
        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

Command	Description
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	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 application-specific integrated circuit (ASIC) and the send and receive statistics for packets reaching the CPU.

show controllers cpu-interface [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is a partial output example from the **show controllers cpu- interface** command:

```
Switch# show controllers cpu-interface
stp packets :950454 retrieved, 0 dropped
ram access packets :18944680 retrieved, 0 dropped
routing protocol packets :170334 retrieved, 0 dropped
forwarding packets :0 retrieved, 0 dropped
routing packets :249 retrieved, 0 dropped
L2 protocol packets :95025 retrieved, 0 dropped
igmp snooping protocol packets :746 retrieved, 0 dropped
queue7 :0 retrieved, 0 dropped
icmp redirect packets :0 retrieved, 0 dropped
icmp unreachable packets :0 retrieved, 0 dropped
logging packets :0 retrieved, 0 dropped
addr learning packets :0 retrieved, 0 dropped
rpffail packets :0 retrieved, 0 dropped
queue13 :50 retrieved, 0 dropped
queue14 :0 retrieved, 0 dropped
queue15 :0 retrieved, 0 dropped
RAM Access:
   11375600 sends   18944688 read replies       2829 write replies
   11375597 completed          0 retries          0 failures
          0 nomem          0 nobuffers          0 errors
          0 expedite toggles          0 fa-lost          0 fa-passives
SCInstance = 0xD9D558
```

```
SCInstance fields:fs_notify_failed = 0, no_fsd_space = 0
           invalid_frames = 0, unexpected_valid_frames = 0
           too_large_frames = 0
           Aged frames from notify queues and unexpected retrieves:
               aged_frames[0] = 0, unexpected_retrieves[0] = 0
               aged_frames[1] = 0, unexpected_retrieves[1] = 0
               aged_frames[2] = 0, unexpected_retrieves[2] = 0
               aged_frames[3] = 0, unexpected_retrieves[3] = 0

<output truncated>

               aged_frames[14] = 0, unexpected_retrieves[14] = 0
               aged_frames[15] = 0, unexpected_retrieves[15] = 0
           sc_cpu_buffer = 0x80000000, sc_regs = 0x81000000
           sc_notify_ram = 0x81010000
CPU Interface registers:
    0x810004A4:storage_congestion_time = 0x10
    0x810004A8:channel_number = 0x102
    0x810004AC:cpu_buffer_control = 0x1
    0x810004B0:current_time = 0x0

<output truncated>

    0x810004FC:notify_overrun_count = 0x0
    0x81000500:notify_ring_control = 0x85
    0x81000504:pci_control = 0x2A00002

<output truncated>
```

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
show interfaces	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 keywords to display the interface internal registers.

show controllers ethernet-controller *interface-id* [**asic** | **phy**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	The physical interface.
asic	(Optional) Display the state of the internal registers on the forwarding application-specific integrated circuit (ASIC) for the interface.
phy	(Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the interface.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for the interface.

When you enter the **asic** or **phy** keyword, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is an example of output from the **show controllers ethernet-controller** command. Table 2-15 describes the *Transmit* fields, and Table 2-16 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet0/2
Transmit GigabitEthernet0/2        Receive
3617834078 Bytes                39726165 Bytes
    419261 Unicast frames         161535 Unicast frames
  82798461 Multicast frames       146421 Multicast frames
     12718 Broadcast frames            1 Broadcast frames
         0 Discarded frames            0 No dest, unicast
         0 Too old frames             43 No dest, multicast
         0 Deferred frames             0 No dest, broadcast
         0  1 collision frames
         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     220108 Minimum size frames
         0  8 collision frames     60959  65 to 127 byte frames
         0  9 collision frames          0 128 to 255 byte frames
         0 10 collision frames      26931 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 14 collision frames          0 Flooded frames
         0 15 collision frames          0 Overrun frames
         0 Excessive collisions        16 VLAN filtered frames
         0 Late collisions              0 Source routed frames
         0 Good (1 coll) frames         0 Valid oversize frames
         0 Good(>1 coll) frames         0 Pause frames
         0 Pause frames                 0 Symbol error frames
         0 VLAN discard frames          0 Invalid frames, too large
         0 Excess defer frames          0 Valid frames, too large
         0 Too large frames             0 Invalid frames, too small
  80469577 64 byte frames               3 Valid frames, too small
   2605574 127 byte frames
     58711 255 byte frames
     26956 511 byte frames
     70222 1023 byte frames
         0 1518 byte frames
```

Table 2-15 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.
Discarded frames	The number of frames dropped on an interface.
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.
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.

Table 2-15 Transmit Field Descriptions (continued)

Field	Description
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.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
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.
Good (>1 coll) frames	The number of frames that are successfully sent on an interface after more than one but less than 15 collisions occur. This value does not include the number of frames that are not successfully sent after more than one collision occurs.
Pause frames	The number of pause frames sent on an interface.
VLAN discard frames	The number of frames dropped on an interface because the CFI[1] bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.
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.

1. CFI = Canonical Format Indicator

Table 2-16 Receive Field Descriptions

Field	Description
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS[1] 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 forwarded to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are forwarded to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are forwarded to broadcast addresses.
No dest, unicast	The total number of frames received with a unicast destination address that cannot be forwarded.
No dest, multicast	The total number of frames received with a multicast destination address that cannot be forwarded.
No dest, broadcast	The total number of frames received with a broadcast destination address that cannot be forwarded.
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.
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.
Flooded frames	The total number of flooded frames received on an interface.
Overrun frames	The total number of overrun frames received on an interface.
VLAN filtered frames	The total number of frames that are filtered because of the VLAN information in the frame, such as an IEEE 802.1Q tag or a VLAN ID other than the IDs configured on the interface. This value does not include frames that are smaller than 64 bytes or larger than the maximum frame size
Source routed frames	The total number of frames received on an interface that are dropped because the source route bit is set in the source address of the native frame. This value includes frames that have a valid FCS value and are between 64 bytes and the maximum allowed frame size.
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.
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.

Table 2-16 Receive Field Descriptions (continued)

Field	Description
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU[2] 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 have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.

1. FCS = frame check sequence
2. MTU = maximum transmission unit

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

show controllers switch

Use the **show controllers switch** privileged user command to display the settings of the resource-allocation priority or the wirespeed-store feature.

show controllers switch {**resource-allocation priority** | **wirespeed-store**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

resource-allocation priority	Display the resource-allocation priority setting.
wirespeed-store	Display the wirespeed setting.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show controllers switch resource-allocation priority** command:

```
Switch> show controllers resource-allocation priority
Switch Priority Resource Allocation is enabled.
```

Related Commands

Command	Description
switchcore resource-allocation priority	Reserves switch resources for high-priority traffic or gives buffer storage more priority than packet retrieval.
switchcore wirespeed-store	

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 application-specific integrated circuits (ASICs) that are CAM controllers.

show controllers tcam [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples

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

```
Switch# show controllers tcam
CAM Controller 1:
  Revision: 5A5A5A00, Control: 0000025F, Status: 00000000.
  CAM 1:
    Revision: 00 00000000 00B30101
    Size: 00 00000000 00080040
    Device ID: 00 00000000 00000000
    Config: 00 00000000 88000002
    ReplyID[0]: 00 00000000 00000000
    ReplyID[1]: 00 00000000 00000000
    ReplyID[2]: 00 00000000 00000000
    ReplyID[3]: 00 00000000 00000000
    Hit Result[0]: 00 00000000 00000000
    Hit Result[1]: 00 00000000 00000000
    Hit Result[2]: 00 00000000 00000000
    Hit Result[3]: 00 00000000 00000000
    Hit Result[4]: 00 00000000 00000000
    Hit Result[5]: 00 00000000 00000000
    Hit Result[6]: 00 00000000 00000000
    Hit Result[7]: 00 E00004E8 40001A63
    Global Mask[10]: FF FFFFFFFF FFFFFFFF
    Global Mask[11]: FF FFFFFFFF FFFFFFFF
    Global Mask[12]: FF FFFFFFFF FFFFFFFF
```

```
    Global Mask[13]: FF FFFFFFFF FFFFFFFF
    Global Mask[14]: FF FFFFFFFF FFFFFFFF
    Global Mask[15]: FF FFFFFFFF FFFFFFFF
    Global Mask[16]: FF FFFFFFFF FFFFFFFF
    Global Mask[20]: FF FFFFFFFF FFFFFFFF
    Global Mask[21]: FF FFFFFFFF FFFFFFFF
    Global Mask[22]: FF FFFFFFFF FFFFFFFF
    Global Mask[23]: FF FFFFFFFF FFFFFFFF
    Global Mask[24]: FF FFFFFFFF FFFFFFFF
    Global Mask[25]: FF FFFFFFFF FFFFFFFF
    Global Mask[26]: FF FFFFFFFF FFFFFFFF
    Global Mask[27]: FF FFFFFFFF FFFFFFFF
    Global Mask[30]: FF FFFFFFFF FFFFFFFF
    Global Mask[31]: FF FFFFFFFF FFFFFFFF
    Global Mask[32]: FF FFFFFFFF FFFFFFFF
    Global Mask[33]: FF FFFFFFFF FFFFFFFF
  CAM 2:
    Revision: 00 00000000 00B30101
    Size: 00 00000000 00080040
    Device ID: 00 00000000 00000001
    Config: 00 00000000 B8000022
    ReplyID[0]: 00 01010101 01010101
    ReplyID[1]: 00 01010101 01010101
   ReplyID[2]: 00 01010101 01010101
   ReplyID[3]: 00 01010101 01010101
   Hit Result[0]: 00 00000000 00000000
   Hit Result[1]: 00 00000000 00000000
   Hit Result[2]: 00 00000000 00000000
   Hit Result[3]: 00 00000000 00000000
   Hit Result[4]: 00 00000000 00000000
   Hit Result[5]: 00 00000000 00000000
   Hit Result[6]: 00 00000000 00000000
   Hit Result[7]: 00 60003880 C00011D3
   Global Mask[10]: FF FFFFFFFF FFFFFFFF
   Global Mask[11]: FF FFFFFFFF FFFFFFFF
   Global Mask[12]: FF FFFFFFFF FFFFFFFF
   Global Mask[13]: FF FFFFFFFF FFFFFFFF
   Global Mask[14]: FF FFFFFFFF FFFFFFFF
   Global Mask[15]: FF FFFFFFFF FFFFFFFF
   Global Mask[16]: FF FFFFFFFF FFFFFFFF
   Global Mask[20]: FF FFFFFFFF FFFFFFFF
   Global Mask[21]: FF FFFFFFFF FFFFFFFF
   Global Mask[22]: FF FFFFFFFF FFFFFFFF

<output truncated>
```

show controllers utilization

Use the **show controllers utilization** user EXEC command to display bandwidth utilization on the switch or specific ports.

show controllers [*interface-id*] **utilization** [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the switch interface.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SE	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show controllers utilization** command.

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Fa0/1              0                    0
Fa0/2              0                    0

<output truncated>

Total Ports : 12
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 fastethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

Table 2-17 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
show controllers ethernet-controller	Displays the interface internal registers.

show dot1q-tunnel

Use the **show dot1q-tunnel** user EXEC command to display information about IEEE 802.1Q tunnel ports.

show dot1q-tunnel [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Specify the interface for which to display IEEE 802.1Q tunneling information. Valid interfaces include physical ports and port channels.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

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

Examples

These are examples of output from the **show dot1q-tunnel** command:

```
Switch> show dot1q-tunnel
LAN Port(s)
-----
Gi0/1
Gi0/2
Gi0/3
Gi0/6
Po2

Switch> show dot1q-tunnel interface gigabitethernet0/1
LAN Port(s)
-----
Gi0/1
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays IEEE 802.1Q native VLAN tagging status.
switchport mode dot1q-tunnel	Configures an interface as an IEEE 802.1Q tunnel port.

show dot1x

Use the **show dot1x** user EXEC command to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified interface.

show dot1x [{**all** [**summary**] | **interface** *interface-id*} [**details** | **statistics**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all [**summary**]	(Optional) Display the IEEE 802.1x status for all ports.
interface *interface-id*	(Optional) Display the IEEE 802.1x status for the specified interface.
details	(Optional) Display the IEEE 802.1x interface details.
statistics	(Optional) Display IEEE 802.1x statistics for the specified port.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	The **all** keyword was added.
12.2(25)SED	The display was expanded to include **auth-fail-vlan** 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)
```

If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify the **statistics** keyword without the **interface** *interface-id* option, statistics appear for all interfaces. If you specify the **statistics** keyword with the **interface** *interface-id* option, statistics appear for the specified interface.

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

Examples

This is an example of output from the **show dot1x** user EXEC 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** user EXEC command:

```
Switch> show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Critical Recovery Delay         100
Critical EAPOL              Disabled

Dot1x Info for FastEthernet0/1
----------------------------------
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

<output truncated>
```

This is an example of output from the **show dot1x all summary** user EXEC command:

```
Interface       PAE     Client          Status
---------------------------------------------------------
Fa0/1           AUTH    none            UNAUTHORIZED
Fa0/2           AUTH    00a0.c9b8.0072  AUTHORIZED
Fa0/3           AUTH    none            UNAUTHORIZED
```

This is an example of output from the **show dot1x interface** *interface-id* user EXEC command:

```
Switch> show dot1x interface fastethernet0/2
Dot1x Info for FastEthernet0/2
----------------------------------
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** user EXEC commmand:

```
Switch# show dot1x interface fastethernet0/2 details
Dot1x Info for FastEthernet0/2
----------------------------------
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 fastethernet0/1 details
Dot1x Info for FastEthernet0/1
----------------------------------
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 2-18 describes the fields in the display.

```
Switch> show dot1x interface fastethernet0/2 statistics
Dot1x Authenticator Port Statistics for FastEthernet0/2
-------------------------------------------
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 2-18 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.
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
dot1x control-direction	Resets the configurable IEEE 802.1x parameters to their default values.

show env

Use the **show env** user EXEC command to display fan, temperature, and power information for the switch.

show env {**all** | **fan** | **power** | **rps** | **temperature**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Display both fan and temperature environmental status.
fan	Display the switch fan status.
power	Display the switch power status.
rps	Display the Redundant Power System (RPS) status.
temperature	Display the switch temperature status.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **power** and **rps** keywords were added.
12.1(12c)EA1	The **fan** and **power** keywords were added.

Usage Guidelines

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

Examples

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

```
Switch> show env all
FAN is FAULTY
TEMPERATURE is OK
```

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

```
Switch> show env power
POWER is OK
```

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

```
Switch> show env rps
RPS is NOT PRESENT
```

show errdisable detect

show errdisable detect [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show errdisable detect
ErrDisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
security-violatio    Enabled
channel-misconfig    Enabled
psecure-violation    Enabled
vmps                 Enabled
loopback             Enabled
unicast-flood        Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
l2ptguard            Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
unicast-flood        Enabled
storm-control        Enabled
ilpower              Enabled
arp-inspection       Enabled
```

Note Though visible in the output, the arp-inspection, ilpower, storm-control, and unicast-flood fields are not valid.

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable flap-values	Displays error condition recognition information.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable flap-values

Use the **show errdisable flap-values** user EXEC command to display conditions that cause an error to be recognized for a cause.

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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
```

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

Examples

This is an example of output from the **show 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
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable detect	Displays error-disable detection status.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disable recovery timer information.

show errdisable recovery [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show 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            Disabled
l2ptguard            Disabled
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)
---------    -----------------    --------------
Gi0/4           link-flap             279
```

Note Though visible in the output, the unicast-flood field is not valid.

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error disable detection status.
show errdisable flap-values	Displays error condition recognition information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

show etherchannel [*channel-group-number*] {**detail** | **load-balance** | **port** | **port-channel** | **summary | protocol**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 64.
detail	Display detailed EtherChannel information.
load-balance	Display the load-balance or frame-distribution scheme among ports in the port channel.
port	Display EtherChannel port information.
port-channel	Display port-channel information.
protocol	Display the protocol that is being used in the EtherChannel.
summary	Display a one-line summary per channel-group.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(14)EA1	The **brief** keyword was removed.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups appear.

In the output, the Passive port list field appears only for Layer 3 port channels. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

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

Examples

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 8
Port-channels: 1 Max Port-channels = 1
               Ports in the group:
               -------------------
Port: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Desirable-Sl     Gcchange = 0
Port-channel  = Po1         GC   = 0x00010001    Pseudo port-channel = Po1
Port index    = 0           Load = 0x00

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.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                              Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/1     SC    U6/S7   H       30s      1        128        Any      16

Partner's information:

          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Gi0/1     vegas-p2             0002.4b29.4600   Gi0/1        9s SC      10001

Age of the port in the current state: 00d:00h:07m:52s
Port: Gi0/2
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Desirable-Sl     Gcchange = 0
Port-channel  = Po1         GC   = 0x00010001    Pseudo port-channel = Po1
Port index    = 0           Load = 0x00

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.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                              Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/2     SC    U6/S7   H       30s      1        128        Any      16

Partner's information:

          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Gi0/2     vegas-p2             0002.4b29.4600   Gi0/2        4s SC      10001

Age of the port in the current state: 00d:00h:07m:55s
               Port-channels in the group:
               ----------------------
```

```
Port-channel: Po1
------------

Age of the Port-channel   = 00d:00h:08m:28s
Logical slot/port   = 1/0           Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse

Ports in the Port-channel:

Index   Load   Port    EC state
------+------+------+------------
  0     00     Gi0/1    desirable-sl
  0     00     Gi0/2    desirable-sl

Time since last port bundled:    00d:00h:07m:56s    Gi0/1
```

This is an example of output from the **show etherchannel 1 protocol** command:

```
Switch# show etherchannel 1 protocol
Protocol:  LACP
```

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
        R - Layer3      S - Layer2
        U - port-channel in use
Group Port-channel  Ports
-----+------------+-----------------------------------------------------------
1     Po1(SU)     Gi0/1(P)   Gi0/2(P)
```

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
------------

Age of the Port-channel   = 00d:00h:10m:41s
Logical slot/port   = 1/0           Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse

Ports in the Port-channel:

Index   Load   Port    EC state
------+------+------+------------
  0     00     Gi0/1    desirable-sl
  0     00     Gi0/2    desirable-sl

Time since last port bundled:    00d:00h:10m:08s    Gi0/1
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet interface to an EtherChannel group.
interface port-channel	Accesses or creates the port channel.

show flowcontrol

Use the **show flowcontrol** user EXEC command to display the flow control status and statistics.

show flowcontrol [**interface** *interface-id* | **module** *module-number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display the flow control status and statistics for a specific interface.
module *module-number*	(Optional) Display the flow control status and statistics for all interfaces. The only valid module-slot value is 0.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(14)EA1	This command was introduced.

Usage Guidelines

Use this command to display the flow control status and statistics on the switch or about a specific interface.

Use the **show flowcontrol** command to display information about all the switch interfaces. The output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module** *module-number* command.

Use the **show flowcontrol interface** *interface-id* command to display information about the Gigabit Ethernet interfaces on the switch.

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

Examples

This is an example of output from the **show 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
<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
---------  -------- -------- -------- --------    ------- -------
Gi0/2      desired  off      off      off         0       0
```

Related Commands

Command	Description
flowcontrol	Sets the receive flow-control state for an interface.

show fm

Use the **show fm** privileged EXEC command to display feature-manager information for a specified port label or VLAN label to list features associated with that label, including if any features were not able to fit in the hardware or if configuration conflicts have occurred. Use the **show fm interface** or **show fm vlan** command to determine the port-label or vlan-label number.

show fm {{**port-label** *label-id*} | {**vlan-label** *label-id*}} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

port-label *label-id*	Port labels are used features configured on a port, such as port ACLs. The range is 0 to 127.
vlan-label *label-id*	VLAN labels are used for features configured on VLANs, such as router ACLs and VLAN maps. The range is 0 to 255.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **label** keyword was replaced by the **port-label** and **vlan-label** keywords.

Usage Guidelines

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

When the output shows *Conflicts exist* with other access groups, there is a configuration conflict with access control lists (ACLs) on the switch. You are trying to apply a port ACL to a switch that already has VLAN maps or input router ACLs applied; or you are trying to apply an input router ACL or VLAN map to a switch that has port ACLs applied.

When the output shows an *unloaded* indicator or no number following the *Loaded into CAM(s):* entry, the feature was not loaded in the hardware. To allocate more system resources to maximize the number of security ACLs that can fit in the hardware, you can use the **sdm prefer access** global configuration command to set the Switch Database Management feature to the access template.

If the output shows a *merge failure*, the **sdm prefer access** global configuration command has no effect.

Examples

You can enter the **show fm interface** privileged EXEC command for an interface to learn the port-label number for the port. You can then enter the **show fm port-label** privileged EXEC command to display more details, as shown in this example:

```
Switch# show fm interface gigabitethernet0/1
Conflicts exist with layer 3 access groups.
Input Port Label:2
Switch# show fm port-label 2
Conflicts exist with layer 3 access groups.
Needed in CAM(s):1
Loaded into CAM(s):1
Sent to CPU by CAM(s):
Interfaces: Gi0/1
IP Access Group:ip3 0 VMRs
DHCP Broadcast Suppression Disabled.
MAC Access Group:(None) 0 VMRs
```

This example of the **show fm port-label 3** output shows that there was not enough room in hardware to load an ACL. Label 3 is needed in CAM 1 but is not loaded in CAM 1; instead, it is sent to the CPU.

```
Switch# show fm port-label 3
Needed in CAM(s):1
Loaded into CAM(s):
Sent to CPU by CAM(s):1
Interfaces: Gi0/3
IP Access Group:100 3400 VMRs
DHCP Broadcast Suppression Disabled.
MAC Access Group:(None) 2 VMRs
```

This is an example of output from the **show fm vlan-label** command when there has been a merge failure on an input access-group:

```
Switch# show fm vlan-label 1
Unloaded due to merge failure or lack of space:
  InputAccessGroup
  Merge Fail:input
Input Features:
  Interfaces or VLANs: Vl1
  Priority:normal
  Vlan Map:(none)
  Access Group:131, 6788 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs:
  Priority:low
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:(none), 0 VMRs
```

This is an example of output from the **show fm vlan-label** command when there was not enough room for an input access group in the hardware:

```
Switch# show fm vlan-label 1
Unloaded due to merge failure or lack of space:
  InputAccessGroup
Input Features:
  Interfaces or VLANs: Vl1
  Priority:normal
  Vlan Map:(none)
  Access Group:bigone, 11 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs:
  Priority:low
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:(none), 0 VMRs
```

This is an example of output from the **show fm vlan-label** command when there was not enough room for the input access group or the output access group on the label. Note that the access groups were configured on two different interfaces. Labels are assigned independently for input and output.

```
Switch# show fm vlan-label 1
Unloaded due to merge failure or lack of space:
  InputAccessGroup OutputAccessGroup
Input Features:
  Interfaces or VLANs: Vl1
  Priority:normal
  Vlan Map:(none)
  Access Group:bigone, 11 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs: Vl2
  Priority:normal
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:bigtwo, 11 VMRs
```

Related Commands

Command	Description
show fm interface	Displays per-interface feature manager information.
show fm vlan	Displays per-VLAN feature manager information.

show fm interface

Use the **show fm interface** privileged EXEC command to display per-interface feature-manager information. Use it with the **show fm port-label** privileged EXEC command to get information about features applied to the interface.

show fm interface *interface-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	Specify an interface; valid interfaces include: • physical interface—type and port number. • port channel—**port-channel** *port-channel-number* (1 to 64). • null—**null 0**. • VLAN—**vlan** *vlan-id* (1 to 4094; do not enter leading zeros). VLAN interfaces are VLANs that have a switch virtual interface (SVI) assigned.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(13)EA1	This command was modified to include policy-based routing (PBR) information.

Usage Guidelines

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

Examples

This is an example of output from the **show fm interface gigabitethernet0/1** command:

```
Switch# show fm interface gigabitethernet0/1
  Conflicts exist with layer 3 access groups.
  Input Port Label:2
```

You can then use the **show fm port-label 2** privileged EXEC command to view more detail.

This is an example of output from the **show fm interface vlan 1** command with PBR enabled on the interface.

```
Switch# show fm interface vlan 1
Input VLAN Label: 1
Output VLAN Label: 0 (default)
Policy Label: 9
Priority: normal
```

Related Commands

Command	Description
show fm	Displays feature-manager information for a specified label and lists configuration conflicts or features associated with that label that were not able to fit into the hardware.
show fm vlan	Displays per-VLAN feature manager information.

show fm vlan

Use the **show fm vlan** privileged EXEC command to display per-VLAN feature-manager information. Use with the **show fm vlan-label** privileged EXEC command to get information about features applied to the VLAN.

show fm vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	Any VLAN ID, whether or not a switch virtual interface (SVI) has been assigned. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show fm vlan 1** command that shows an ACL configuration conflict. It displays the VLAN label used in hardware for VLAN feature configuration.

```
Switch# show fm vlan 1
Conflicts exist with layer 2 access groups.
Input VLAN Label:1
Output VLAN Label:0 (default)
Priority:normal
```

Related Commands

Command	Description
show fm interface	Displays per-interface feature manager information.
show fm	Displays feature-manager information for a specified label and lists configuration conflicts or features associated with that label that were not able to fit into the hardware.

show forward

Use the **show forward** privileged EXEC command for an interface to determine how the hardware would forward a frame that matches the specified parameters.

show forward *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* [**ex-class**] [**ex-l4op**] [**ex-qos**] [**ex-sig**] [| {**begin** | **exclude** | **include**} *expression*]

show forward *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* [**ip** *src-ip dst-ip* [*protocol-num*] [**adjacency** *adjacency_index*] [**dscp** *dscp*] [**frag** *fragment*] [**option**] | {**icmp** *icmp-type icmp-code*} | {**igmp** *igmp-version igmp-type*} | {**tcp** *src-port dst-port flags*} | {**udp** *src-port dst-port*}] [**ex-class**] [**ex-l4op**] [**ex-qos**] [**ex-sig**] [| {**begin** | **exclude** | **include**} *expression*]

show forward *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* **sap** *lsap* [**cos** *cos*] [**ex-class**] [**ex-l4op**] [**ex-qos**] [**ex-sig**] [| {**begin** | **exclude** | **include**} *expression*]

show forward *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* [**arpa** *ethertype* | **snap** *snap_type*] [**cos** *cos*] [**ex-class**] [**ex-l4op**] [**ex-qos**] [**ex-sig**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	The input physical interface.
vlan *vlan-id*	(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. You should specify the input VLAN even for access ports.
src-mac	48-bit source MAC address.
dst-mac	48-bit destination MAC address.
ex-class	(Optional) Display detailed packet processing information related to classification.
ex-l4op	(Optional) Display detailed packet processing information related to Layer 4 operations.
ex-qos	(Optional) Display detailed packet processing information related to quality of service (QoS).
ex-sig	(Optional) Display detailed packet processing information related to the part of the hardware that recognizes frame formats (signature tables).
ip *src-ip dst-ip*	(Optional) Source and destination IP addresses in dotted decimal notation.
protocol-num	The numeric value of the protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), 89 is Open Shortest Path First (OSPF). If is TCP, UDP, ICMP, or IGMP, you should use the appropriate keyword instead of a numeric value.
adjacency *adjacency_index*	(Optional) Hardware adjacency to be used when a route has more than one adjacency as with multipath routes. The range is from 0 to 7.
dscp *dscp*	(Optional) Differentiated services code point (DSCP) field in the IP header. The range is 0 to 63.
frag *fragment*	(Optional) Two-byte IP fragment field in the IP header. This field includes the Don't Fragment bit (0x4000), the More Fragments bit (0x2000), and the Fragment Offset (0x0 through 0x1FFF). The default is 0x0 (unfragmented packet).

option	(Optional) Keyword signifying IP options are present in the packet.
icmp *icmp-type icmp-code*	Internet Control Message Protocol (ICMP) parameters. The *icmp-type* and *icmp-code* ranges are 0 to 255.
igmp *igmp-version igmp-type*	Internet Group Management Protocol (IGMP) parameters. The *igmp-version* and *igmp-type* ranges are 0 to 255.
tcp *src-port dst-port flags*	TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte. The *src-port* and *dst-port* ranges are 0 to 65535.
udp *src-port dst-port*	User Datagram Protocol (UDP) parameters. The *src-port* and *dst-port* ranges are 0 to 65535.
cos *cos*	(Optional) Class of service (CoS) value of the frame. The range is 0 to 1024.
arpa *ethertype*	(Optional) Address Resolution Protocol (ARP) Ethernet II encapsulation type and the Ethertype field. The range is 0 to 65535.
snap *snap_type*	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type and the Ethertype field. The range is 0 to 65535.
sap *lsap*	(Optional) Service access point (SAP) encapsulation type and the LSAP field. The range is 0 to 65535.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If you enter this command without any arguments, you enter a dialog mode. This mode is not operational in this release.

Because of the many and varied items that go into the forwarding decision, this command requires detailed information about the frame in order to correctly indicate how the hardware would forward the frame.

This command has limited ability to account for QoS settings. It does not take into account any packet arrival rates, so if the system has been configured to mark down or police traffic based on data arrival rates, the command will display inaccurate information for traffic that exceeds the configured rates.

If QoS or ACLs are not configured, and if no port-channel interfaces are present, the most important parameters to specify are source interface, source VLAN, destination MAC address, and destination IP address (if applicable). The output is likely to be accurate, even if other parameters are missing or estimated.

If port channel interfaces are present, it is important to specify the source MAC address and IP address correctly.

If ACLs are present, all keywords in the command could be important to the forwarding decision.

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

Examples

Following are three examples of outputs from the **show forward** command. Table 2-19 describes the major sections in the output display.

In this example, the destination MAC address is the router's MAC address and routing lookups are performed:

```
Switch# show forward fastethernet0/1 vlan 8 0000.1111.2222 0022.3355.8800 ip 8.8.8.10
4.4.4.33 255
signature:00000007, comparison ind:10, control info:2000941A control map:00000000
vlan:8, vlanid entry:000C0012 00000000 00000000 04400000
adjptr:D  adjacency:E0002409 00000404 04210000
vlan:1033, vlanid entry:0004000A 00000000 00000000 00000000
vlan:1033, vlanid entry:0004000A 00000000 00000000 00000000

lookup  key                                 bk adata    rawoff secoff sec
qos     960808080A04040421 800000000000FF0000 0  00000000 006304 004064  4
acl     960808080A04040421 800000000000FF0000 1  00000082 045408 002016  1
route   420808080A04040421 000000000000000000 0  3FFF800D 006361 000025  3
learn   187008000011112222 901208000004040421 0  80010003 002176 002176  0
forw    187008000011112222 901208000004040421 1  40020000 043328 010560  5
outacli A60808080A04040421 800000000000FF0000 0  00000083 012448 002016  2

bridgeDestMap:  00000000 00000000 0000FFFF FFFFFFC7
vlanMask:       00000000 00000000 0000FFFF EFFFFFFF
sourceMask:     00000000 00000000 00000000 00000000
globalMap:      00000000 00000000 00000000 00000000
globalMask:     00000000 00000000 0002FFFF EFFFFC03
forwMap:        00000000 00000000 00000000 10000000

frame notifies:
src u_dat vlan fl q-map
2   00    8    01 00000000 00000000 00000000 10000000

Egress q 44
signature:00000007, comparison ind:10, control info:2000941A control map:00000000
vlan:8, vlanid entry:000C0012 00000000 00000000 00000000
adjptr:D  adjacency:E0002409 00000404 04210000
vlan:1033, vlanid entry:0004000A 00000000 88000000 00000000

lookup  key                                 bk adata    rawoff secoff sec
route   420808080A04040421 000000000000000000 0  3FFF800D 006361 000025  3
GigabitEthernet0/1 vlan 1033, dst 0000.0404.0421 src 0022.3355.8800, cos 0x0, dscp 0x0
```

In this example, the destination MAC address is not the router's MAC address. No routing lookups are performed:

```
Switch# show forward fastethernet0/1 vlan 8 0000.1111.2222 0022.3355.9800 ip 8.8.8.10
4.4.4.33 255
signature:00000007, comparison ind:10, control info:2000941A control map:00000000
vlan:8, vlanid entry:000C0012 00000000 00000000 04620000
vlan:8, vlanid entry:000C0012 00000000 00000000 04620000

lookup  key                                bk adata    rawoff secoff sec
qos     940808080A04040421 800000000000FF0000 0  00000000 006304 004064  4
acl     940808080A04040421 800000000000FF0000 1  00000082 045408 002016  1
learn   187008000011112222 801008002233559800 0  80010003 002176 002176  0
forw    187008000011112222 801008002233559800 1  40020000 043328 010560  5

bridgeDestMap:  00000000 00000000 0000FFFF FFFFFFC7
vlanMask:       00000000 00000000 0000FFFF FFFFFE7F
portMask:       00000000 00000000 00000000 00000080
sourceMask:     00000000 00000000 00000000 00000000
globalMap:      00000000 00000000 00000000 00000000
globalMask:     00000000 00000000 0002FFFF EFFFFC03
forwMap:        00000000 00000000 00000000 00000100

frame notifies:
src u_dat vlan fl q-map
2   00    8    00 00000000 00000000 00000000 00000100

Egress q 8
signature:00000007, comparison ind:10, control info:2000941A control map:00000000
vlan:8, vlanid entry:000C0012 00000000 00000000 04620000
FastEthernet0/2 vlan 8, dst 0022.3355.9800 src 0000.1111.2222, cos 0x0, dscp 0x0
```

This is an example of the display that results if one of the destinations for the packet is the switch CPU. Note that in this case the section after the *frame notifies* section is labeled *Cpu q* and that a queue name appears:

```
Switch# show forward fastethernet0/1 vlan 7 0000.1111.2222 0022.3355.8800 ip 1.1.1.1
7.7.7.1 255
signature:00000007, comparison ind:11, control info:2000941A control map:00000000
vlan:7, vlanid entry:000C0011 00000000 00318C60 88000000
adjptr:0  adjacency:00000000 00000000 0000C000
vlan:7, vlanid entry:000C0011 00000000 00318C60 88000000

lookup  key                                bk adata    rawoff secoff sec
qos     960101010107070701 800000000000FF0000 0  00000000 006304 004064  4
acl     960101010107070701 800000000000FF0000 1  00000082 045408 002016  1
route   420101010107070701 000000000000000000 0  00048000 006345 000009  3
learn   186007000011112222 800E08002233558800 0  80010003 002176 002176  0
forw    186007000011112222 800E08002233558800 1  40090000 033000 000232  5

bridgeDestMap:  00000000 00000000 00000000 00000000
routeDestMap:   00000000 00000000 00100000 00000000
sourceMask:     00000000 00000000 00000000 00000000
globalMap:      00000000 00000000 00000000 00000000
globalMask:     00000000 00000000 0002FFFF EFBFFC03
forwMap:        00000000 00000000 00100000 00000000

frame notifies:
src u_dat vlan fl q-map
2   00    7    01 00000000 00000000 00100000 00000000

Cpu q:100 - routing queue
```

Table 2-19 show forward Output Description

Output Section	Description
General (no heading) Includes the first few lines of the display.	Displays lookup results for several tables in the input portion of the hardware. The output includes packet formats, the configuration of the input VLAN, and other information.
lookup section	Describes TCAM lookups performed during the input forwarding decision and the results of these lookups.
Bitmaps and masks	Displays maps and masks used to calculate the final set of forwarding destinations.
frame notifies section	Contains the bitmap that results from combining the maps and masks from the bitmaps section. If SPAN is configured, there might be additional bitmaps displayed.
Egress q <nn> section	There is an egress section for each separate destination port. The output is varied, but the important information is in the line containing the name of an output interface, output VLAN ID, and rewritten destination MAC address for the frame. If the output interface is a trunk port that needs to send multiple copies of the frame on different VLANs (for example, for IP multicast frames), several lines might contain the same output interface name, but a different output VLANs. If output security ACLs are present, it is possible that one or more of these *egress q* sections will not contain a line listing an output port. This happens when the output ACL denies the packet.
Cpu q <nn> <name> section	When the CPU is one of the destinations for a packet, this section appears, followed by a queue name. This name should correspond to one of the queue names in the output from the **show controllers cpu-interface** privileged EXEC command, where statistics appear for the number of packets received at each queue.

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** {*module-number*}] | **counters** | **description** | **etherchannel** | **flowcontrol** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** {*module-number*}] | **trunk**] | [**transceiver properties** | **detail**] [**module** {*module-number*} | **trunk**] | [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Display accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(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.
module *module-number*	(Optional) Display **capabilities**, **switchport** configuration, or **transceiver** characteristics (depending on preceding keyword) of all interfaces on the The range is 1 to 9. This option is not available if you entered a specific interface ID.
counters	(Optional) See the **show interfaces counters** command.
description	(Optional) Display the administrative status and description set for an interface.
etherchannel	(Optional) Display interface EtherChannel information.
flowcontrol	(Optional) Display interface flowcontrol information
pruning	(Optional) Display interface trunk VTP pruning information.
stats	(Optional) Display the input and output packets by switching path for the interface.
status	(Optional) Display the status of the interface. A status of *unsupported* in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
err-disabled	(Optional) Display interfaces in error-disabled state.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
backup	(Optional) Display Flex Link backup interface configuration and status for the specified interface.
transceiver [**detail** | **properties**]	(Optional) Display the physical properties of a CWDM[1] or DWDM[2] small form-factor (SFP) module interface. The keywords have these meanings: • **detail**—(Optional) Display calibration properties, including high and low numbers and any alarm information. • **properties**—(Optional) Display speed, duplex, and inline power settings on an interface.

trunk	Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

1. coarse wavelength-division multiplexer
2. dense wavelength-division multiplexer

Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **private-vlan mapping**, **random-detect**, **rate-limit**, and **shape** keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(12c)EA1	The **capabilities** keyword was added.
12.1(22)EA1	The **transceiver** and **properties** keywords were added.
12.2(22)SEE	The **counters**, **backup**, **detail**, and **trunk** keywords were added.

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module** *number* command to display the capabilities of all interfaces on that switch. If there is no switch with that module number, there is no output.
- 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.
- Use the **show interface switchport module** *number* command to display the switch port characteristics of all interfaces on that switch. If there is no switch with that module number, there is no output.

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

Examples

This is an example of output from the **show interfaces gigabitethernet0/1** command:

```
Switch# show interfaces gigabitethernet0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 0002.4b29.4401 (bia 0002.4b29.4401)
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7122 packets input, 783062 bytes, 0 no buffer
     Received 5137 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     9222 packets output, 2188728 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 1 deferred
     0 lost carrier, 0 no carrier
     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       1073      69828        325      31868
                     ARP          6        384          2        120
Vlan10
                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
          Spanning Tree          8        480        326      19560
                    CDP         28      10920         29      11513
GigabitEthernet0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/3
                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:

```
Switch# show interfaces fastethernet0/1 capabilities
FastEthernet0/1
  Model:                 WS-C3550G-48-EI
  Type:                  10/100BaseTX
  Speed:                 10,100,auto
  Duplex:                half,full,auto
  UDLD:                  yes
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(none),tx-(none)
  Fast Start:            yes
  CoS rewrite:           yes
  ToS rewrite:           yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            Yes
  Dot1x:                 Yes
```

This is an example of output from the **show interfaces gigabitethernet0/4 description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```
Switch# show interfaces gigabitethernet0/4 description
Interface Status         Protocol Description
G10/4     up             down     Connects to Marketing
```

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 gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2     up             down     Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
----
GigabitEthernet0/9:
Port state    = Down Not-in-Bndl
Channel group = 6           Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Pseudo port-channel = Po6
Port index    = 0           Load = 0x00

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.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                              Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/9     d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 14d:12h:32m:05s
----
GigabitEthernet0/10:
Port state    = Up Sngl-port-Bndl Mstr Not-in-Bndl
Channel group = 10          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x000A0001    Pseudo port-channel = Po10
Port index    = 0           Load = 0x00

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.
        d - PAgP is down.

Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                              Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/10          U4/S4   H       30s      0        128        Any      0

Age of the port in the current state: 01d:06h:05m:59s
----
Port-channel6:
Age of the Port-channel   = 01d:06h:05m:38s
Logical slot/port   = 1/1           Number of ports = 0
```

```
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
----
Port-channel10:
Age of the Port-channel   = 01d:06h:06m:15s
Logical slot/port   = 1/0           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 flowcontrol** command. Table 2-20 lists the fields in this display.

```
Switch# show interfaces flowcontrol
Port    Send FlowControl  Receive FlowControl  RxPause TxPause
        admin    oper     admin    oper
-----   -------- -------- -------- --------    ------- -------
Fa0/1   Unsupp.  Unsupp.  off      off         0       0
Fa0/2   Unsupp.  Unsupp.  off      off         0       0
<output truncated>
Gi0/1   desired  off      off      off         0       0
Gi0/2   desired  off      off      off         0       0
Po1     Unsupp.  Unsupp.  off      off         0       0
Po2     Unsupp.  Unsupp.  off      off         0       0
Po59    Unsupp.  Unsupp.  off      off         0       0
Po60    Unsupp.  Unsupp.  off      off         0       0
Po63    Unsupp.  Unsupp.  off      off         0       0
Po64    Unsupp.  Unsupp.  off      off         0       0
```

Table 2-20 show interfaces flowcontrol Field Descriptions

Field	Description
Port	Displays the port name.
Send FlowControl	
Admin	Displays the administrative (configured) setting for the flow control **send** mode.
Oper	Displays the operational (running) setting for the flow control **send** mode.
Receive FlowControl	
Admin	Displays the administrative (configured) setting for the flow control **receive** mode.
Oper	Displays the operational (running) setting for the flow control **receive** mode.
RxPause	Displays the number of pause frames received.
TxPause	Displays the number of pause frames sent.
On	Flow control is enabled.
Off	Flow control is disabled.
Desired	Flow control is enabled if the other end supports it.
Unsupp.	Flow control is not supported.

This is an example of output from the **show interfaces gigabitethernet0/1 pruning** command when pruning is enabled in the VTP domain:

```
Switch# show interfaces gigibitethernet0/1 pruning
```

```
Port    Vlans pruned for lack of request by neighbor
Gi0/1   3,4

Port    Vlans traffic requested of neighbor
Gi0/1   1-3
```

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

```
Switch# show interface gigabitethernet0/1 stats
GigabitEthernet0/1
    Switching path    Pkts In   Chars In   Pkts Out  Chars Out
    Processor            7790    1122034         23       1938
    Route cache             0          0          0          0
    Total                7790    1122034         23       1938
```

This is an example of output from the **show interfaces status** command. It displays the status of all interfaces.

```
Switch# show interfaces status

Port    Name               Status       Vlan       Duplex  Speed Type
Gi0/1   CubeA              connected    1          a-full  a-100 10/100/1000Base TX
Gi0/2   CubeC              notconnect   1            auto   auto 10/100/1000Base TX
Gi0/3   CubeE              disabled     1            auto   auto 10/100/1000Base TX
Gi0/4   CubeG              notconnect   1            auto   auto 10/100/1000Base TX
Gi0/5   CubeI              notconnect   routed       auto   auto 10/100/1000Base TX
Gi0/6   CubeK              notconnect   routed       auto   auto 10/100/1000Base TX
Gi0/7   CubeM              notconnect   1            auto   auto 10/100/1000Base TX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in error-disabled state.

```
Switch# show interfaces status err-disabled

Port    Name               Status       Reason
Gi0/4                      notconnect   link-flap

informational error message when the timer expires on a cause
---------------------------------------------------------------

5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Gi0/4
```

This is an example of output from the **show interfaces switchport** command for a single interface. Table 2-21 describes the fields in the display.

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
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
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 2-21 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 Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	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.
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 Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
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.

This is an example of output from the **show interfaces gigabitethernet0/1 trunk** command. It displays trunking information for the interface.

```
Switch# show interfaces gigabitethernet0/1 trunk

Port      Mode         Encapsulation  Status        Native vlan
Gi0/1     desirable    negotiate      not-trunking  1

Port      Vlans allowed on trunk
Gi0/1     1

Port      Vlans allowed and active in management domain
Gi0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1
```

This is an example of output from the **show interfaces transceiver properties** command. If you do not specify an interface, the output of the command shows the status on all switch ports:

```
Switch# show interfaces transceiver properties
Name : Fa0/1
Administrative Speed: auto 10 100
Administrative Duplex: auto
Administrative Auto-MDIX: N/A
Administrative Power Inline: enable
Operational Speed: 100
Operational Duplex: full
Operational Auto-MDIX: N/A

Name : Fa0/2
Administrative Speed: auto 10
Administrative Duplex: auto
Administrative Auto-MDIX: N/A
Administrative Power Inline: enable
Operational Speed: auto
Operational Duplex: auto
Operational Auto-MDIX: N/A

<output truncated>
```

This is an example of output from the **show interfaces module** *module-number* **transceiver properties** command for a specific interface:

```
Switch# show interfaces fastethernet0/1 transceiver properties
Name : Fa0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: N/A
Administrative Power Inline: disable
Operational Speed: 100
Operational Duplex: full
Operational Auto-MDIX: N/A
```

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
     ------------------------------------------------------------
     Fa1/0/1             Fa1/0/2             Active Up/Backup Standby
     Fa3/0/3             Fa4/0/5             Active Down/Backup Up
     Po1                 Po2                 Active Standby/Backup Up
```

Related Commands

Command	Description
switchport access	Configures a port as a static-access or dynamic-access port.
switchport block	Blocks unknown unicast or multicast traffic on an interface.
switchport broadcast	Configures the VLAN membership mode of a port.
switchport protected	Isolates unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch.
switchport trunk pruning	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*] **counters** [**errors** | **etherchannel** | **protocol status** | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type and slot and port number.
errors	(Optional) Display error counters.
etherchannel	(Optional) Display EtherChannel counters.
protocol status	(Optional) Display the current status of enabled protocols.
trunk	(Optional) Display trunk counters.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **module** and *vlan-id* keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(25)SE	The **etherchannel** and **protocol status** keywords were added and the **broadcast**, **multicast**, and **unicast** keywords were removed.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

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

Examples

This is an example of output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi0/1           23324617          10376         185709         126020
Gi0/2                  0              0              0              0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi0/1            4990607         28079         21122             10
Gi0/2            1621568         25337             0              0

Switch# show interfaces counters errors

    Port        Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize
    Gi0/1               0          0          0          0         0
    Gi0/2               0          0          0          0         0
    Gi0/3               0          0          0          0         0
    Gi0/4               0          0          0          0         0


    Port      Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen     Runts    Giants
    Gi0/1              0         0         0          0         0         0       0
    Gi0/2              0         0         0          0         0         0       0
    Gi0/3              0         0         0          0         0         0       0
    Gi0/4              0         0         0          0         0         0       0
```

This is an example of output from the **show interfaces counters protocol status** command for all interfaces.

```
Switch# show interfaces counters protocol status
Protocols allocated:
 Vlan1: Other, IP
 Vlan1001: Other, IP, ARP
 FastEthernet0/1: Other, IP
 FastEthernet0/2: Other, IP, Spanning Tree, ARP, CDP
 FastEthernet0/3: Other, IP
 FastEthernet0/4: Other, IP
 FastEthernet0/5: Other, IP
 FastEthernet0/6: Other, IP
 FastEthernet0/7: Other, IP

<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
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show inventory

Use the **show inventory** user EXEC command to display product identification (PID) information for the hardware.

show inventory [*entity-name* | **raw**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

entity-name	(Optional) Display the specified entity. For example, enter the interface (such as **gigabitethernet1/0/1**) into which a small form-factor pluggable (SFP) module is installed.
raw	(Optional) Display every entity in the device.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEC	This command was introduced.

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 displays the entity location (slot identity), entity description, and the UDI (PID, VID, and SN) of that entity.

Note If there is no PID, no output is displayed when a user enters the **show inventory** command.

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

Examples

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

```
Switch# show inventory
NAME: "sw-1-3-f48", DESCR: "Cisco Catalyst 3550 48 10/100 baseT ports + 2 Gig uplinks
fixed configuration Layer 2/3 Ethernet Switch"
PID: WS-C3550-48      , VID: C0 , SN: CHK0614V09S
```

show arp access-list

Use the **show arp access-list** user EXEC command to display detailed information about Address Resolution Protocol (ARP) access control lists (ACLs).

show arp access-list [*acl-name*] [| {**begin** | **exclude** | **include**} *expression*]

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

acl-name	(Optional) Name of the ACL.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show arp access-list** 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
```

Related Commands

Command	Description
arp access-list	Defines an ARP ACL.
deny (ARP access-list configuration)	Denies an ARP packet based on matches against the Dynamic Host Configuration Protocol (DHCP) bindings.
ip arp inspection filter vlan	Permits ARP requests and responses from a host configured with a static IP address.
permit (ARP access-list configuration)	Permits an ARP packet based on matches against the DHCP bindings.

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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interfaces [*interface-id*]	(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.
log	(Optional) Display the configuration and contents of the dynamic ARP inspection log buffer.
statistics [**vlan** *vlan-range*]	(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.
vlan *vlan-range*	(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.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

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

Examples

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 gigabitethernet0/1
 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
 2000              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

 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
arp access-list	Defines an ARP ACL.
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
clear ip arp inspection statistics	Clears the dynamic ARP inspection statistics.
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
ip arp inspection vlan logging	Controls the type of packets that are logged per VLAN.
show arp access-list	Displays detailed information about ARP access lists.

show ip dhcp snooping

Use the **show ip dhcp snooping** user EXEC command to display the DHCP snooping configuration.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced
12.2(25)SEE	The command output was updated to show the global suboption configuration.

Usage Guidelines

This command displays only the results of global configuration. Therefore, in this example, the circuit ID suboption appears in its default format of **vlan-mod-port**, even if a string is configured for the circuit ID.

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
    circuit-id format: vlan-mod-port
    remote-id format: string
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/5              yes         unlimited
FastEthernet0/7              yes         unlimited
FastEthernet0/3              no          5000
FastEthernet0/5              yes         unlimited
FastEthernet0/7              yes         unlimited
FastEthernet0/5              yes         unlimited
FastEthernet0/7              yes         unlimited
```

Related Commands

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

show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** user EXEC command to display the DHCP snooping binding table and configuration information for all interfaces on a switch.

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

ip-address	(Optional) Specify the binding entry IP address.
mac-address	(Optional) Specify the binding entry MAC address.
interface *interface-id*	(Optional) Specify the binding input interface.
vlan *vlan-id*	(Optional) Specify the binding entry VLAN.
| begin	Display begins with the line that matches the *expression*.
| exclude	Display excludes lines that match the *expression*.
| include	Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced
12.2(25)SE	The **dynamic** and **static** keywords were removed.

Usage Guidelines

The **show ip dhcp snooping binding** command output shows the dynamically configured bindings.

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

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

Examples

This 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 an interface:

```
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 2-22 describes the fields in the **show ip dhcp snooping binding** command output.

Table 2-22 show ip dhcp snooping binding Command Output

Field	Description
MAC Address	Client hardware MAC address
IP Address	Client IP address assigned from the DHCP server
Lease (seconds)	IP address lease time
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 **Note** 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
show ip dhcp snooping	Displays the DHCP snooping configuration.

show ip dhcp snooping database

Use the **show ip dhcp snooping database** user EXEC command to display the status of the DHCP snooping binding database agent.

show ip dhcp snooping database [**detail**] **[** | **{begin** | **exclude** | **include**} ***expression***]

This command is available only if your switch is running the IP services image, formerly known as the enhanced multilayer image (EMI).

Syntax Description

detail	(Optional) Display detailed status and statistics information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

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 Succeded 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 Succeded 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
ip dhcp snooping	Enables DHCP snooping on a VLAN.
ip dhcp snooping database	Configures the DHCP snooping binding database agent or the binding file.
show ip dhcp snooping	Displays DHCP snooping information.

show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to view all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

show ip igmp profile [*profile number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

profile number	(Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles appear.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

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

Examples

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
```

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.

show ip igmp snooping

Use the **show ip igmp snooping** user EXEC command 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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

groups	(Optional) See the **show ip igmp snooping groups** command.
mrouter	(Optional) See the **show ip igmp snooping mrouter** command.
querier	(Optional) See the **show ip igmp snooping querier** command.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(19)EA1	The **group** and **querier** keywords were added.
12.2(25)SE	The **groups** keyword was added, and the **group** keyword was removed.
12.2(25)SEA	The **detail** keyword was added.

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.

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

Examples

This is an example of output from the **show ip igmp snooping** command. It shows how to display 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>
```

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows how to display 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

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
```

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
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping last-member-query-interval	Enables the IGMP snooping configurable-leave timer.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
ip igmp snooping report-suppression	Enables IGMP report suppression.
ip igmp snooping source-only-learning age-timer	Enables and configures the aging time of the forward-table entries that the switch learns by using the source-only learning method.
ip igmp snooping tcn	Configures the IGMP topology change notification behavior.
ip igmp snooping tcn flood	Specifies multicast flooding as the IGMP spanning-tree topology change notification behavior.
ip igmp snooping vlan immediate-leave	Enables IGMP snooping immediate-leave processing on a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port or configures the multicast learning method.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping groups	Displays the IGMP snooping multicast table for the switch.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

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** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
dynamic	(Optional) Display entries learned by IGMP snooping.
user	Optional) Display only the user-configured multicast entries.
ip_address	(Optional) Display characteristics of the multicast group with the specified group IP address.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SE	This command was introduced.

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.

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

Examples

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

```
Switch# show ip igmp snooping groups

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/2
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/2
```

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

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

This is an example of output from the **show ip igmp snooping groups 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
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1
104       224.1.4.3       igmp        v2          Gi0/1
```

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

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan mrouter	Configures a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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.

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

Examples

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

```
Switch> show ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
  1          Gi0/1,Gi0/1, Router
  2          Gi0/3,Gi0/4
```

This is an example of output from the **show ip igmp snooping mrouter vlan 1** command. It shows how to display multicast router ports for a specific VLAN.

```
Switch# show ip igmp snooping mrouter vlan 1
vlan            ports
-----+---------------------------------------
  1          Gi0/1,Gi0/1, Router
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port.
ip igmp snooping vlan static	Statically adds a Layer 2 port as a member of a multicast group.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN
show ip igmp snooping groups	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** user EXEC command 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**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

detail	Optional) Display detailed IGMP querier information.
vlan *vlan-id* [**detail**]	Optional) Display IGMP querier information for the specified VLAN. The range is 1 to 1001 and 1006 to 4094. Use the **detail** keyword to display detailed information.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Examples

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

```
Switch> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  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             Fa8/0/1

Global IGMP switch querier status
-----------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10

Vlan 1:   IGMP switch querier status

-----------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
-----------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping querier	Enables the IGMP querier function in Layer 2 networks.
show ip igmp snooping	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** user EXEC command 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*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

ip-address	(Optional) Display IP source bindings for a specific IP address.
mac-address	(Optional) Display IP source bindings for a specific MAC address.
dhcp-snooping	(Optional) Display IP source bindings that were learned by DHCP snooping.
static	(Optional) Display static IP source bindings.
interface *interface-id*	(Optional) Display IP source bindings on a specific interface.
vlan *vlan-id*	(Optional) Display IP source bindings on a specific VLAN.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

The **show ip source binding** command output shows the dynamically and statically configured bindings in the Dynamic Host Configuration Protocol (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
```

Related Commands

Command	Description
ip dhcp snooping binding	Configures the DHCP snooping binding database.
ip source binding	Configures static IP source bindings on the switch.

show ip verify source

Use the **show ip verify source** user EXEC command to display the IP source guard configuration on the switch or on a specific interface.

show ip verify source [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Display IP source guard configuration on a specific interface.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Examples

This is an example of output from the **show ip verify source** command:

```
Switch> show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
Fa0/1      ip           active       10.0.0.1                         10
Fa0/1      ip           active       deny-all                         11-20
Fa0/2      ip           inactive-trust-port
Fa0/3      ip           inactive-no-snooping-vlan
Fa0/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
Fa0/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
Fa0/4      ip-mac       active       deny-all         deny-all        12-20
Fa0/5      ip-mac       active       10.0.0.3         permit-all      10
Fa0/5      ip-mac       active       deny-all         permit-all      11-20
```

In the previous example, this is the IP source guard configuration:

- On the Fast Ethernet 0/1 interface, Dynamic Host Configuration Protocol (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 list (ACL) is applied on the interface for the VLANs on which IP source guard is not configured.
- The Fast Ethernet 0/2 interface is configured as trusted for DHCP snooping.
- On the Fast Ethernet 0/3 interface, DHCP snooping is not enabled on the VLANs to which the interface belongs.
- On the Fast Ethernet 0/4 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 Fast Ethernet 0/5 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 fastethernet0/6
IP source guard is not configured on the interface fa0/6.
```

Related Commands

Command	Description
ip verify source	Enables IP source guard on an interface.

show l2protocol-tunnel

Use the **show l2protocol-tunnel** user EXEC command to display information about Layer 2 protocol tunnel ports. Displays information for interfaces with protocol tunneling enabled.

show l2protocol-tunnel [**interface** *interface-id*] [**summary**] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Specify the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 64.
summary	(Optional) Display only Layer 2 protocol summary information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

After enabling Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the **l2protocol-tunnel** interface configuration command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

If you enter the **show l2protocol-tunnel** [**interface** *interface-id*] command, only information about the active ports on which all the parameters are configured appears.

If you enter the **show l2protocol-tunnel summary** command, only information about the active ports on which some or all of the parameters are configured appears.

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

Examples

This is an example of output from the **show l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5

Port    Protocol Shutdown  Drop      Encapsulation Decapsulation Drop
                 Threshold Threshold Counter       Counter       Counter
------- -------- --------- --------- ------------- ------------- -------------
Fa0/10  ---           ----      ----          ----          ----          ----
        stp           ----      ---- 9847          1866          0
        vtp           ----      ---- 77            12            0
        pagp          ----      ---- 859           860           0
        lacp          ----      ---- 0             0             0
        udld          ----      ---- 219           211           0
Fa0/11  cdp           1100      ---- 2356          2350          0
        stp           1100      ---- 116           13            0
        vtp           1100      ---- 3             67            0
        pagp          ----       900 856           5848          0
        lacp          ----       900 0             0             0
        udld          ----       900 0             0             0
Fa0/12  cdp           ----      ---- 2356          0             0
        stp           ----      ---- 11787         0             0
        vtp           ----      ---- 81            0             0
        pagp          ----      ---- 0             0             0
        lacp          ----      ---- 849           0             0
        udld          ----      ---- 0             0             0
Fa0/13  cdp           ----      ---- 2356          0             0
        stp           ----      ---- 11788         0             0
        vtp           ----      ---- 81            0             0
        pagp          ----      ---- 0             0             0
        lacp          ----      ---- 849           0             0
        udld          ----      ---- 0             0             0
```

This is an example of output from the **show l2protocol-tunnel summary** command:

```
Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5

Port    Protocol    Shutdown         Drop            Status
                    Threshold        Threshold
                    (cdp/stp/vtp)    (cdp/stp/vtp)
                    (pagp/lacp/udld) (pagp/lacp/udld)
------- ----------- ---------------- ---------------- ----------
Fa0/10  --- stp vtp ----/----/----   ----/----/----   up
     pagp lacp udld ----/----/----   ----/----/----
Fa0/11  cdp stp vtp 1100/1100/1100   ----/----/----   up
     pagp lacp udld ----/----/----    900/ 900/ 900
Fa0/12  cdp stp vtp ----/----/----   ----/----/----   up
     pagp lacp udld ----/----/----   ----/----/----
Fa0/13  cdp stp vtp ----/----/----   ----/----/----   up
     pagp lacp udld ----/----/----   ----/----/----
Fa0/14  cdp stp vtp ----/----/----   ----/----/----   down
     pagp ---- udld ----/----/----   ----/----/----
Fa0/15  cdp stp vtp ----/----/----   ----/----/----   down
     pagp ---- udld ----/----/----   ----/----/----
Fa0/16  cdp stp vtp ----/----/----   ----/----/----   down
     pagp lacp udld ----/----/----   ----/----/----
Fa0/17  cdp stp vtp ----/----/----   ----/----/----   down
     pagp lacp udld ----/----/----   ----/----/----
```

Related Commands

Command	Description
clear l2protocol-tunnel counters	Clears counters for protocol tunneling ports.
l2protocol-tunnel	Enables Layer 2 protocol tunneling for CDP, STP, or VTP packets on an interface.
l2protocol-tunnel cos	Configures a class of service (CoS) value for tunneled Layer 2 protocol packets.

show l2tcam

Use the **show l2tcam** privileged EXEC command to display information about the portion of the ternary content addressable memory (TCAM) devoted to Layer 2 addresses. Use the keywords to display forwarding (bridging) or learning (MAC address learning) information or to display allocation statistics of MAC address types.

show l2tcam {**cam** {**forwarding** [*entry-id*] **learning**} | **shadow**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

cam	Display contents and associated information about TCAM Layer 2 contents. This display output is a raw hex dump of information, intended for a Cisco technical support representative.
forwarding	Display TCAM Layer 2 forwarding (bridging) information.
entry-id	Number from 0 to 4294967295 identifying a forwarding entry.
learning	Display TCAM Layer 2 learning (MAC address learning) information.
shadow	Display allocation statistics for various address types of MAC addresses that the software keeps track of. Address types are identified only by number.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is an example of output from the **show l2tcam cam learning** command:

```
Switch# show l2tcam cam learning
mask 1156  F7 FFFFFFFF FFFFFFFF
mask 1157  F7 FFFFFFFF FFFFFFFF
mask 1158  F7 FFFFFFFF FFFFFFFF
mask 1159  F7 FFFFFFFF FFFFFFFF
9248       00 00000000 00000000     80070000
9249       00 00000000 00000000     80060000
9250       00 00000000 00000000     80070000
9251       18 00010002 4B293A00     80020000
9252       00 00000000 00000000     80060000
9253       00 00000000 00000000     80010000
9254       00 00000000 00000000     80030000
9255       18 00010002 4B296700     80040000
<output truncated>

 9368       FF FFFFFFFF FFFFFFFF     5E731478
9369       FF FFFFFFFF FFFFFFFF     17B195AE
9370       FF FFFFFFFF FFFFFFFF     AB2DECEA
9371       FF FFFFFFFF FFFFFFFF     D821EC4E
9372       FF FFFFFFFF FFFFFFFF     E6E55344
9373       FF FFFFFFFF FFFFFFFF     FBFB0EEE
9374       FF FFFFFFFF FFFFFFFF     2057A03D
9375       FF FFFFFFFF FFFFFFFF     E55FE7C3
```

This is an example of output from the **show l2tcam shadow** command:

```
Switch# show l2tcam shadow
learning table
type  start  end   firstfree  firstfreeentry  flag  used/free
0     0      79    0          0               4        0/640
1     80     83    80         0               4        0/32
2     1159   84    1159       3               2        3/8605
3     1160   1167  1160       0               1        0/64
4     1168   1171  1168       1               1        1/31

forwarding table
type  start  end   firstfree  firstfreeentry  flag  used/free
0     0      0     0          0               12       0/0
1     0      0     0          0               12       0/0
2     0      77    0          0               4        0/624
3     78     83    82         6               1       38/10
4     84     1159  84         3               4        3/8605
5     1287   1160  1275       3               2       99/925
6     1415   1288  1403       3               2       99/925
7     1416   1417  1416       0               1        0/16
8     1801   1418  1801       0               2        0/3072
9     1802   1803  1802       1               1        1/15
10    1804   1805  1804       1               1        1/15
11    1809   1806  1809       0               2        0/32
12    1810   1811  1810       2               1        2/14
```

Related Commands

Command	Description
show l3tcam	Displays information about the TCAM devoted to Layer 3 forwarding information.
show mac address-table	Displays the MAC address table static and dynamic entries.

show l3tcam

Use the **show l3tcam** privileged EXEC command to display information about the portion of the ternary content addressable memory (TCAM) devoted to Layer 3 forwarding (IP routing) information.

show l3tcam {**cam** | **shadow**} [| **{begin | exclude | include}** *expression*]

Syntax Description

cam	Display contents and associated information about TCAM Layer 3 contents devoted to unicast and multicast IP routing. This display output is a raw hex dump of information, intended for a Cisco technical support representative.
shadow	Display contents and associated information about TCAM Layer 3 contents formatted to display routes and adjacencies associated with each mask, and some overall statistics.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

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

Examples

This is an example of output from the **show l3tcam cam** command:

```
Switch# show l3tcam cam
C2 00 00 00 00 00 00 00 00
Mask(s)
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00
F1 00 00 00 00 FF FF FF FF - 80 07 00 00 00 00 00 00 00

Entries
C2 00 00 00 00 00 00 00 00 - 80 00 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 FF FF FF FF - 80 00 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 00 00 00 00 - 80 01 00 00 00 00 00 00 00          ( 00 04 80 00 )
```

```
C2 00 00 00 00 FF FF FF FF - 80 01 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 00 00 00 00 - 80 02 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 FF FF FF FF - 80 02 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 08 08 00 08 - 80 00 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 08 08 01 08 - 80 01 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 08 08 02 08 - 80 02 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 08 08 0A 08 - 80 00 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 08 08 0B 08 - 80 01 00 00 00 00 00 00 00          ( 00 04 80 00 )
C2 00 00 00 00 08 08 0C 08 - 80 02 00 00 00 00 00 00 00          ( 00 04 80 00 )

<output truncated>
```

This is an example of output from the **show l3tcam shadow** command:

```
Switch# show l3tcam shadow
L3 TCAM:total words = 30720, used words = 194

Prefix 34:Start=0(0) End=15(127) FirstFree=98, NumFree = 30

Offset  Tbl+Flg SA              DA              Lbl Assoc
============================================================
Mask    0xF1    0.0.0.0         255.255.255.255   7 --

     0  0xC2    0.0.0.0         0.0.0.0           0 0x00048000 (CPU)
     2  0xC2    0.0.0.0         255.255.255.255   0 0x00048000 (CPU)
     4  0xC2    0.0.0.0         0.0.0.0           1 0x00048000 (CPU)
     6  0xC2    0.0.0.0         255.255.255.255   1 0x00048000 (CPU)
     8  0xC2    0.0.0.0         0.0.0.0           2 0x00048000 (CPU)
    10  0xC2    0.0.0.0         255.255.255.255   2 0x00048000 (CPU)
    12  0xC2    0.0.0.0         8.8.0.8           0 0x00048000 (CPU)
    14  0xC2    0.0.0.0         8.8.1.8           1 0x00048000 (CPU)
    16  0xC2    0.0.0.0         8.8.2.8           2 0x00048000 (CPU)
    18  0xC2    0.0.0.0         8.8.10.8          0 0x00048000 (CPU)
    20  0xC2    0.0.0.0         8.8.11.8          1 0x00048000 (CPU)
    22  0xC2    0.0.0.0         8.8.12.8          2 0x00048000 (CPU)
    24  0xC2    0.0.0.0         10.10.10.40       0 0x00048000 (CPU)
    26  0xC2    0.0.0.0         10.10.0.0         0 0x00048000 (CPU)
    28  0xC2    0.0.0.0         10.10.255.255     0 0x00048000 (CPU)
    30  0xC2    0.0.0.0         38.0.0.8          1 0x00048000 (CPU)

<output truncated>
```

Related Commands

Command	Description
show adjacency	Displays Cisco Express Forwarding (CEF) adjacency table information. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Switching Services Command Reference, Release 12.2**.
show arp	Displays the entries in the ARP table. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2**.
show ip route	Displays the current state of the routing table. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2**.
show l2tcam	Displays information about the portion of the TCAM devoted to Layer 2 information.

show lacp

Use the **show lacp** user EXEC command to display Link Aggregation Control Protocol (LACP) channel-group information.

show lacp {*channel-group-number* {**counters** | **internal** | **neighbor**} | {**counters** | **internal** | **neighbor** | **sys-id**}} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 6.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
sys-id	Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and a MAC address.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active port-channel information. To display the nonactive information, enter the **show lacp** command with a group number.

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

Examples

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

```
Switch> show lacp counters
LACPDUs         Marker      Marker Response    LACPDUs
Port        Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------
Channel group:1
Fa0/5       19     10       0      0        0      0         0
Fa0/6       14     6        0      0        0      0         0
Fa0/7       8      7        0      0        0      0         0
```

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

```
Switch> show lacp 1 internal
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 1
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Fa0/5     SP      indep     32768         0x1       0x1     0x4      0x7C
Fa0/6     SP      indep     32768         0x1       0x1     0x5      0x7C
Fa0/7     SP      down      32768         0x1       0x1     0x6      0xC
```

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

```
Switch> show lacp 1 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 1 neighbors

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Fa0/5     00000,0000.0000.0000  0x0             85947s        SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          0                     0x0             0x0

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Fa0/6     00000,0000.0000.0000  0x0             86056s        SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          0                     0x0             0x0

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Fa0/7     00010,0008.a343.b580  0x6             86032s        SA

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x1             0x35
```

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

Related Commands

Command	Description
clear lacp	Clears the LACP channel-group information.

show mac access-group

Use the **show mac access-group** user EXEC command to display the MAC access control lists (ACLs) configured for an interface or a switch.

show mac access-group [**interface** *interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(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 64.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; the **interface** keyword is available only in privileged EXEC mode.

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mac-access group** user EXEC command. In this display, 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
Interface GigabitEthernet0/5:
   Inbound access-list is not set

<output truncated>

Interface GigabitEthernet0/10:
   Inbound access-list is not set
Interface GigabitEthernet0/11:
   Inbound access-list is not set
Interface GigabitEthernet0/12:
   Inbound access-list is not set
```

This is an example of output from the **show mac access-group interface gigabitethernet0/2** command:

```
Switch# show mac access-group interface gigabitethernet0/2
Interface GigabitEthernet0/2:
   Inbound access-list is macl_e1
```

Related Commands

Command	Description
mac access-group	Applies a MAC access group to an interface.

show mac address-table

Use the **show mac address-table** user EXEC command with no keywords to display the MAC address table static and dynamic entries.

show mac address-table [**|** {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table** command replaces the **show mac-address-table** command (with the hyphen).

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table** command was replaced by the **show mac address-table** command.

Usage Guidelines

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

Examples

This is an example of output from the **show mac address-table** command:

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
All    0000.0000.0001    STATIC     CPU
All    0000.0000.0002    STATIC     CPU
All    0000.0000.0003    STATIC     CPU
All    0000.0000.0009    STATIC     CPU
All    0000.0000.0012    STATIC     CPU
All    0180.c200.000b    STATIC     CPU
All    0180.c200.000c    STATIC     CPU
All    0180.c200.000d    STATIC     CPU
All    0180.c200.0010    STATIC     CPU
   1    0030.9441.6327    DYNAMIC    Fa0/23
Total Mac Addresses for this criterion: 9
```

Related Commands

Command	Description
clear mac address-table dynamic	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.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table address

Use the **show mac address-table address** user EXEC command to display MAC address table information for the specified MAC address.

show mac address-table address *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*] [| **{begin | exclude | include}** ***expression*****]**

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table address** command replaces the **show mac-address-table address** command (with the hyphen).

Syntax Description

mac-address	Specify the 48-bit MAC address; the valid format is H.H.H.
interface *interface-id*	(Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for the specific VLAN only. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table address** command was replaced by the **show mac address-table address** command.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table aging-time

Use the **show mac address-table aging-time** user EXEC command to display the aging time in all VLANs or the specified VLAN.

show mac address-table aging-time [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table aging-time** command replaces the **show mac-address-table aging-time** command (with the hyphen).

Syntax Description

vlan *vlan-id*	(Optional) Display aging time information for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table aging-time** command was replaced by the **show mac address-aging-time** command.

Usage Guidelines

If no VLAN number is specified, the aging time for all VLANs appears.

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

Examples

This is an example of output from the **show 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
```

Related Commands

Command	Description
mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table count

Use the **show mac address-table count** user EXEC command to display the number of addresses present in all VLANs or the specified VLAN.

show mac address-table count [**vlan** *vlan-id*] [| {**begin | exclude | include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table count** command replaces the **show mac-address-table count** command (with the hyphen).

Syntax Description

vlan *vlan-id*	(Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table count** command was replaced by the **show mac address-table count** command.

Usage Guidelines

If no VLAN number is specified, the address count for all VLANs appears.

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

Examples

This is an example of output from the **show 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
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table dynamic

Use the **show mac address-table dynamic** user EXEC command to display dynamic MAC address table entries only.

show mac address-table dynamic [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table dynamic** command replaces the **show mac-address-table dynamic** command (with the hyphen).

Syntax Description

address *mac-address*	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H.
interface *interface-id*	(Optional) Specify an interface to match; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table dynamic** command was replaced by the **show mac address-table dynamic** command.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
clear mac address-table dynamic	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.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table interface

Use the **show mac address-table interface** user EXEC 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*] [**|** {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table interface** command replaces the **show mac-address-table interface** command (with the hyphen).

Syntax Description

interface-id	Specify an interface type; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table interface** command was replaced by the **show mac address-table interface** command.

Usage Guidelines

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

Examples

This is an example of output from the **show 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
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table multicast

Use the **show mac address-table multicast** user EXEC command to display the Layer 2 multicast entries for all VLANs. Use the command in privileged EXEC mode to display specific multicast entries.

show mac address-table multicast [**count**] | **igmp-snooping** [**count**] | **user** [**count**] | **vlan** [**count**] | [*vlan-id* [**count**] | **igmp-snooping** [**count**] | **user** [**count**]] [| {**begin** | **exclude** | **include**} *expression*]

Note The **show mac address-table multicast** command only shows non-IP multicast addresses. Use the **show ip igmp snooping multicast** user EXEC command to display IP multicast addresses.

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table multicast** command replaces the **show mac-address-table multicast** command (with the hyphen).

Syntax Description

count	(Optional) Display the total number of entries for the specified command options instead of the actual entries.
igmp-snooping	(Optional) Display entries learned through Internet Group Management Protocol (IGMP) snooping.
user	(Optional) Display only the user-configured multicast entries.
vlan *vlan-id*	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table multicast** command was replaced by the **show mac address-table multicast** command.

Usage Guidelines

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

Examples

This is an example of output from the **show mac address-table multicast** command. It shows how to display all multicast entries for the switch.

```
Switch> show mac address-table multicast
Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.5e00.0128  IGMP    Gi0/1
```

This is an example of output from the **show mac address-table multicast count** command. It shows how to display a total count of MAC address entries for the switch.

```
Switch> show mac address-table multicast count

Multicast MAC Entries for all vlans:    10
```

This is an example of output from the **show mac address-table multicast vlan 1 count** command. It shows how to display a total count of MAC address entries for a VLAN.

```
Switch> show mac address-table multicast vlan 1 count

Multicast MAC Entries for vlan 1:    4
```

This is an example of output from the **show mac address-table multicast interface vlan1** command. It shows how to display the user-configured multicast entries for VLAN 1.

```
Switch> show mac address-table multicast interface vlan1
vlan   mac address     type         ports
-----+---------------+--------+---------+---+--------------------------------
  1  0100.5e02.0203    user           Gi0/1,Gi0/2
  1  0100.5e00.0128    user           Gi0/1,Gi0/2
```

This is an example of output from the **show mac address-table multicast vlan 1 igmp-snooping count** command. It shows how to display the total number of entries learned through IGMP snooping for VLAN 1:

```
Switch> show mac address-table multicast vlan 1 igmp-snooping count
Number of IGMP Learned Multicast Addresses:    2
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.

Command	Description
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table notification

Use the **show mac address-table notification** user EXEC command to display the MAC address notification settings for all interfaces or the specified interface.

show mac address-table notification [**interface** [*interface-id*] [**|** {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table notification** command replaces the **show mac-address-table notification** command (with the hyphen).

Syntax Description

interface	(Optional) Display information for all interfaces. Valid interfaces include physical ports and port channels.
interface-id	(Optional) Display information for the specified interface. Valid interfaces include physical ports and port channels.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table notification** command was replaced by the **show mac address-table notification** command.

Usage Guidelines

Use the **show mac address-table notification** command without any keywords to display whether the 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 **interface** keyword to display the flags for all interfaces. If the *interface-id* is included, only the flags for that interface appear.

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

Examples

This is an example of output from the **show mac address-table notification** command:

```
Switch> show mac address-table notification
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

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table static

Use the **show mac address-table static** user EXEC command to display static MAC address table entries only.

show mac address-table static [[**address** *mac-address* [**interface** *interface-id* | **vlan** *vlan-id*]] | [**interface** *interface-id* [**vlan** *vlan-id*]] | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table static** command replaces the **show mac-address-table static** command (with the hyphen).

Syntax Description

address *mac-address*	(Optional) Specify a 48-bit MAC address; the valid format is H.H.H.
interface *interface-id*	(Optional) Specify an interface to match; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table static** command was replaced by the **show mac address-table static** command.

Usage Guidelines

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

Examples

This is an example of output from the **show 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.c200.0002  STATIC  CPU
 All    0180.c200.0003  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: 10
```

Related Commands

Command	Description
mac address-table static	Adds static addresses to the MAC address table.
mac address-table static drop	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table vlan

Use the **show mac address-table vlan** user EXEC command to display the MAC address table information for the specified VLAN.

show mac address-table vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

Note Beginning with Cisco IOS Release 12.1(11)EA1, the **show mac address-table vlan** command replaces the **show mac-address-table vlan** command (with the hyphen).

Syntax Description

vlan-id	(Optional) Display addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **show mac-address-table vlan** command was replaced by the **show mac address-table vlan** command.

Usage Guidelines

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

Examples

This is an example of output from the **show 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.c200.0004  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
Total Mac Addresses for this criterion: 8
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table multicast	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.

show mls qos

Use the **show mls qos** user EXEC command to display global quality of service (QoS) configuration information.

show mls qos [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show mls qos
Qos is enabled
```

Related Commands

Command	Description
mls qos	Enables quality of service (QoS) for the entire switch.

show mls qos aggregate-policer

Use the **show mls qos aggregate-policer** user EXEC command to display the quality of service (QoS) aggregate policer configuration. 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.

show mls qos aggregate-policer [*aggregate-policer-name*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

aggregate-policer-name	(Optional) Display the policer configuration for the specified name.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mls qos aggregate-policer** command:

```
Switch> show mls qos aggregate-policer policer1
aggregate-policer policer1 88000 2000000 exceed-action drop
Not used by any policy map
```

Related Commands

Command	Description
mls qos aggregate-policer	Defines policer parameters that can be shared by multiple classes within a policy map.

show mls qos interface

Use the **show mls qos interface** user EXEC command to display quality of service (QoS) information at the interface level.

show mls qos interface [*interface-id*] [**buffers** | **policers** | **queueing** | **statistics**]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Display QoS information for the specified interface. Valid interfaces include physical ports.
buffers	(Optional) Display buffer settings of the queues. For Gigabit-capable Ethernet ports, the display includes the queue depth for each of the four queues and the tail drop or Weighted Random Early Detection (WRED) thresholds. For 10/100 Ethernet ports, the display includes the configured minimum-reserve settings.
policers	(Optional) Display all the policers configured on the interface, their settings, and the number of policers that are currently unassigned.
queueing	(Optional) Display queueing strategy (weighted round robin, priority queueing), the weights corresponding to the queues, and the class of service (CoS)-to-egress-queue map.
statistics	(Optional) Display all the Differentiated Services Code Points (DSCPs) for which statistics are maintained and the corresponding ingress and egress statistics, including the number of bytes dropped.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If no keyword is specified with the **show mls qos interface** command, the display shows the port trusted mode (DSCP trusted, CoS trusted, untrusted, and so forth), the default CoS value, the DSCP-to-DSCP-mutation map (if any) attached to the port, and the policy map (if any) attached to the interface. If a specific interface is not specified, the information for all interfaces appears.

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

Examples

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

```
Switch# show mls qos interface fastethernet0/1
FastEthernet0/1
trust state: not trusted
trust mode: trust cos
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
trust device: cisco-phone
```

This is an example of output from the **show mls qos interface gigabitethernet0/1 buffers** command:

```
Switch> show mls qos interface gigabitethernet0/1 buffers
GigabitEthernet0/1
Notify Q depth:
qid-size
 1 - 25
 2 - 25
 3 - 25
 4 - 25
qid WRED thresh1 thresh2
 1  dis   100      100
 2  dis   100      100
 3  dis   100      100
 4  dis   100      100
```

In the preceding display, the qid-size section shows the weight (the amount of space allocated to each queue) as configured by the **wrr-queue queue-limit** interface configuration command. The next section of the display shows the settings of the tail-drop thresholds for all four queues. The WRED column shows that it is disabled, which means that tail drop is in effect. Tail-drop thresholds are configured by using the **wrr-queue threshold** interface configuration command.

This is an example of output from the **show mls qos interface fastethernet0/1 buffers** command:

```
Switch> show mls qos interface fastethernet0/1 buffers
FastEthernet0/1
Minimum reserve buffer size:
 100 100 100 100 100 100 100 100
Minimum reserve buffer level select:
 4 2 5 7
```

This sample shows that the buffer size for all minimum-reserve levels is set to 100 packets. The last line of the display shows that queue 1 selects minimum-reserve level 4, queue 2 selects minimum-reserve level 2, queue 3 selects minimum-reserve level 5, and queue 4 selects minimum-reserve level 7.

This is an example of output from the **show mls qos interface gigabitethernet0/1 queueing** command:

```
Switch> show mls qos interface gigabitethernet0/1 queueing
GigabitEthernet0/1
Ingress expedite queue: dis
Egress expedite queue: ena
wrr bandwidth weights:
qid-weights
 1 - 25
 2 - 25
 3 - 25
```

```
Dscp-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
      1 :    01 01 01 01 01 01 01 01 01 01
      2 :    01 01 01 01 01 01 01 01 01 01
      3 :    01 01 01 01 01 01 01 01 01 01
      4 :    01 01 01 01 01 01 01 01 01 01
      5 :    01 01 01 01 01 01 01 01 01 01
      6 :    01 01 01 01
Cos-queue map:
cos-qid
 0 - 1
 1 - 1
 2 - 2
 3 - 2
 4 - 3
 5 - 3
 6 - 4
 7 - 4
```

In the preceding display, the egress expedite queue is enabled. Because of this, the weight of the expedite queue (queue 4) is ignored and not used in the ratio calculation. Only the bandwidth weights for the remaining queues appear. The bandwidth weight of the queues is configured by the **wrr-queue bandwidth** interface configuration command. The CoS-to-queue map shows the CoS values that are mapped to select a queue; this map is configured by the **wrr-queue cos-map** interface configuration command.

This is an example of output from the **show mls qos interface gigabitethernet0/1 statistics** command. Table 2-23 describes the fields in this display.

```
Switch> show mls qos interface gigabitethernet0/1 statistics
Ingress
  dscp: incoming   no_change  classified policed    dropped (in bytes)
    1 : 0          0          0          0          0
    2 : 0          0          0          0          0
    3 : 0          0          0          0          0
    45: 0          0          0          0          0
    23: 0          0          0          0          0
Others: 203216935  24234242   178982693  0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in bytes)
   1 : 0             n/a        n/a       0          0
   2 : 0             n/a        n/a       0          0
   3 : 0             n/a        n/a       0          0
   45: 0             n/a        n/a       0          0
   23: 0             n/a        n/a       0          0
Others: 155983       n/a        n/a       0          0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         1024
   4 : 0          0         1024
```

Table 2-23 show mls qos interface statistics Field Descriptions

	Field	Description
Ingress	incoming	Number of packets or bytes with a specific DSCP entering the ingress QoS process.
	no_change	Number of packets or bytes for which the DSCP value did not change after classification.
	classified	Number of packets or bytes classified to this DSCP value.
	policed	Number of packets or bytes marked down from this DSCP value.
	dropped (in bytes)	Number of packets or bytes dropped by policing.
Egress	incoming	Number of packets or bytes with a specific DSCP entering the egress QoS process.
	no_change	Number of packets with a specific DSCP that did not change.
	classified	Number of packets with a specific DSCP that were classified according to the class map.
	policed	Number of packets or bytes marked down from this DSCP.
	dropped (in bytes)	Number of packets or bytes of this DSCP dropped.
WRED drop counts	qid	Queue number.
	thresh1 and thresh2	Number of DSCPs of a specific value dropped at threshold 1 and threshold 2.
	FreeQ	Amount of free queue space available per queue.

Related Commands

Command	Description
mls qos monitor	Defines up to 16 DSCP values for which byte or packet statistics are gathered by hardware.

show mls qos maps

Use the **show mls qos maps** user EXEC command to display quality of service (QoS) mapping information. Maps are used to generate an internal Differentiated Services Code Point (DSCP) value, which represents the priority of the traffic.

show mls qos maps [**cos-dscp** | **dscp-cos** | **dscp-mutation** *dscp-mutation-name* | **dscp-switch-priority** | **ip-prec-dscp** | **policed-dscp**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

cos-dscp	(Optional) Display class of service (CoS)-to-DSCP map.
dscp-cos	(Optional) Display DSCP-to-CoS map.
dscp-mutation *dscp-mutation-name*	(Optional) Display the specified DSCP-to-DSCP-mutation map.
dscp-switch-priority	(Optional) Display the DSCP-to-switch-priority map.
ip-prec-dscp	(Optional) Display the IP-precedence-to-DSCP map.
policed-dscp	(Optional) Display the policed-DSCP map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show mls qos maps** command:

```
Switch> 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 02 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

Dscp-switch priority map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 00
      1 :    00 00 00 00 00 00 01 01 01 01
      2 :    01 01 01 01 01 01 01 01 01 01
      3 :    01 01 02 02 02 02 02 02 02 02
      4 :    02 02 02 02 02 02 02 02 03 03
      5 :    03 03 03 03 03 03 03 03 03 03
      6 :    03 03 03 03

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-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
```

Note The d1 column specifies the most-significant digit in the internal DSCP; the d2 row specifies the least-significant digit in the internal DSCP. The intersection of the d1 and d2 values provides the policed-DSCP, the CoS, the switch priority, or the mutated-DSCP value. For example, in the DSCP-to-CoS map, an internal DSCP value of 43 corresponds to a CoS value of 5.

Related Commands

Command	Description
mls qos map	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.

show monitor

Use the **show monitor** user EXEC command to display Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) session information.

show monitor [**session** {*session_number* | **all** | **local** | **range** | **remote**}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

session *session_number*	(Optional) Specify the number of the SPAN or RSPAN session. The range is 1 to 2.
all	Specify all sessions.
local	Specify local sessions.
range	Specify a range of sessions.
remote	Specify remote sessions.
| begin	Display begins with the line that matches the *expression*.
| exclude	Display excludes lines that match the *expression*.
| include	Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(6)EA1	This command was introduced.
12.1(11)EA1	The **all**, **local**, and **remote** keywords were added.
12.1(13)EA1	The **range** keyword was added.

Usage Guidelines

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

Examples

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

```
Switch# show monitor session 1
Session 1
---------
Type: Local Source Session
Source Ports:
    RX Only:  Fa0/13
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
    Encapsulation: DOT1Q
    Ingress:Enabled, default VLAN=5
Reflector Ports: None
Filter VLANs:      None
Dest RSPAN VLAN: None
```

Related Commands

Command	Description
monitor session	Starts a new SPAN or RSPAN session, adds or deletes interfaces or VLANs to or from an existing SPAN or RSPAN session, and filters SPAN source traffic to specific source VLANs.

show mvr

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

show mvr [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **interface** and **members** keywords are appended to the command.
show mvr members	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. Use the command with keywords to display MVR parameters for a specific receiver port.

show mvr interface [*interface-id* [**members** [**vlan** *vlan-id*]]] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Display MVR type, status, and Immediate Leave setting for the interface.
members	(Optional) Display all MVR groups to which the specified interface belongs.
vlan *vlan-id*	(Optional) Display all MVR group members on this VLAN. The range is from 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

```
Switch# show mvr interface
Port    Type            Status          Immediate Leave
----    ----            -------         ---------------
Gi0/1   SOURCE          ACTIVE/UP       DISABLED
Gi0/2   RECEIVER        ACTIVE/DOWN     DISABLED
Gi0/5   RECEIVER        ACTIVE/UP       ENABLED
```

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 gigabitethernet0/2** command:

```
Switch# show mvr interface gigabitethernet0/2
Type: RECEIVER Status: ACTIVE Immediate Leave: DISABLED
```

This is an example of output from the **show mvr interface gigabitethernet0/1 members** command:

```
Switch# show mvr interface gigabitethernet0/1 members
239.255.0.0     DYNAMIC ACTIVE
239.255.0.1     DYNAMIC ACTIVE
239.255.0.2     DYNAMIC ACTIVE
239.255.0.3     DYNAMIC ACTIVE
239.255.0.4     DYNAMIC ACTIVE
239.255.0.5     DYNAMIC ACTIVE
239.255.0.6     DYNAMIC ACTIVE
239.255.0.7     DYNAMIC ACTIVE
239.255.0.8     DYNAMIC ACTIVE
239.255.0.9     DYNAMIC ACTIVE
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr members	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*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

ip-address	(Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Switch# show mvr members
MVR Group IP    Status          Members
------------    ------          -------
239.255.0.1     ACTIVE          Gi0/1(d), Gi0/5(s)
239.255.0.2     INACTIVE        None
239.255.0.3     INACTIVE        None
239.255.0.4     INACTIVE        None
239.255.0.5     INACTIVE        None
239.255.0.6     INACTIVE        None
239.255.0.7     INACTIVE        None
239.255.0.8     INACTIVE        None
239.255.0.9     INACTIVE        None
239.255.0.10    INACTIVE        None

<output truncated>

239.255.0.255   INACTIVE        None
239.255.1.0     INACTIVE        None
```

This is an example of output from the **show mvr members 239.255.0.2** command. It shows how to view the members of the IP multicast group 239.255.0.2:

```
Switch# show mvr members 239.255.0.2
239.255.0.2     ACTIVE          Gi0/1(d), Gi0/2(d), Gi0/3(d),
                                Gi0/4(d), Gi0/5(s)
```

Related Commands

Command	Description
mvr (global configuration)	Enables and configures multicast VLAN registration on the switch.
mvr (interface configuration)	Configures MVR ports.
show mvr	Displays the global MVR configuration on the switch.
show mvr interface	Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **members** keyword is appended to the command.

show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**} [| {**begin** | **exclude** | **include**} *expression*]]

Syntax Description

channel-group-number	(Optional) Number of the channel group.The range is 1 to 64.
counters	Display traffic information.
internal	Display internal information.
neighbor	Display neighbor information.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

You can enter any **show pagp** command to display the active port channel information. To display the nonactive information, enter the **show pagp** command with a 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
  Gi0/1    45     42       0      0
  Gi0/2    45     41       0      0
```

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
Gi0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi0/2     SC    U6/S7   H       30s      1        128        Any      16
```

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.
   Gi0/1     vegas-p2             0002.4b29.4600   Gi0/1        9s SC      10001
   Gi0/2     vegas-p2             0002.4b29.4600   Gi0/2       24s SC      10001
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.

show parser macro

Use the **show parser macro** user EXEC command to display the parameters for all configured macros or for one macro on the switch.

show parser macro [{**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Display the name of each macro.
description [**interface** *interface-id*]	(Optional) Display all macro descriptions or the description of a specific interface.
name *macro-name*	(Optional) Display information about a single macro identified by the macro name.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(19)EA1	The command was introduced.

Usage Guidelines

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

Examples

This is a partial output example from the **show parser macro** command. The output for the Cisco-default macros varies depending on the switch platform and the software image running on the switch:

```
Switch# show parser macro
Total number of macros = 6
------------------------------------------------------------
Macro name : cisco-global
Macro type : default global
# Enable dynamic port error recovery for link state
# failures
errdisable recovery cause link-flap
errdisable recovery interval 60

<output truncated>

------------------------------------------------------------
Macro name : cisco-desktop
Macro type : default interface
# macro keywords $AVID
# Basic interface - Enable data VLAN only
```

```
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

------------------------------------------------------------------
Macro name : cisco-phone
Macro type : default interface
# Cisco IP phone + desktop template
# macro keywords $AVID $VVID
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID
switchport mode access

<output truncated>

------------------------------------------------------------------
Macro name : cisco-switch
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Do not apply to EtherChannel/Port Group
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

<output truncated>

------------------------------------------------------------------
Macro name : cisco-router
Macro type : default interface
# macro keywords $NVID
# Access Uplink to Distribution
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID

<output truncated>

------------------------------------------------------------------
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

------------------------------------------------------------------
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name standard-switch10
Macro name : standard-switch10
Macro type : customizable
macro description standard-switch10
# Trust QoS settings on VOIP packets
auto qos voip trust
# Allow port channels to be automatically formed
channel-protocol pagp
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
    default global   : cisco-global
    default interface: cisco-desktop
    default interface: cisco-phone
    default interface: cisco-switch
    default interface: cisco-router
    customizable     : snmp
```

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

```
Switch# show parser macro description
Global Macro(s): cisco-global
Interface    Macro Description(s)
------------------------------------------------------------
Fa0/1        standard-switch10
Fa0/2       this is test macro
------------------------------------------------------------
```

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

```
Switch# show parser macro description interface fastethernet0/2
Interface    Macro Description
------------------------------------------------------------
Fa0/2      this is test macro
------------------------------------------------------------
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show running-config	Displays the current operating configuration, including defined macros. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2** > **File Management Commands** > **Configuration File Management Commands**.

show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define classification criteria for incoming traffic. Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

show policy-map [*policy-map-name* [**class** *class-map-name*]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

policy-map-name	(Optional) Display the specified policy-map name.
class *class-map-name*	(Optional) Display QoS policy actions for an individual class.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **interface** keyword is not supported, and the statistics shown in the display should be ignored.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(6)EA1	The **class** keyword was added.

Usage Guidelines

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

Examples

This is an example of output from the **show policy-map** command:

```
Switch> show policy-map
Policy Map policy1
  class  class1
   set dscp 7

Policy Map policy3
  class  class99
   police 96000 999999 exceed-action drop
  class  class3
   police 8000 98989 exceed-action drop
  class  class20
   police 8000 9090 exceed-action drop
  class  class21
   police 904000 9090909 exceed-action policed-dscp-transmit
  class  class22
   police 904000 9090909 exceed-action policed-dscp-transmit
```

Related Commands

Command	Description
mls qos cos policy-map	Defines the class of service (CoS) value of a port in a policy map.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.

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 [**address**] [**interface** *interface-id* [**address** | **vlan**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

address	(Optional) Display all secure MAC addresses on all ports or a specified port.
interface *interface-id*	(Optional) Display port security settings for the specified interface.
address	(Optional) Display port security settings for the specified interface and MAC address.
vlan	(Optional) Display port security settings for all VLANs on the specified interface. This keyword is only visible on interfaces that have the switchport mode set to **trunk**.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(14)EA1	The **vlan** keyword was added.

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 **show port-security** command displays port security settings for the interface.

If you enter an *interface-id* and **vlan**, the **show port-security** command displays the maximum number of secure addresses for the interface and the VLAN.

If you enter the **address** keyword, the **show port-security address** 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 **show port-security interface** *interface-id* **address** 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.

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

Examples

This is an example of the output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
------------------------------------------------------------------------------

     Fa0/1           11            11            0            Shutdown
     Fa0/5           15            5             0            Restrict
     Fa0/11          5             4             0            Protect
------------------------------------------------------------------------------

Total Addresses in System :21
Max Addresses limit in System :6176
```

This is an example of output from the **show port-security interface fastethernet0/2** command:

```
Switch# show port-security interface fastethernet0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 20 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses      : 11
Total MAC Addresses        : 11
Configured MAC Addresses   : 3
Sticky MAC Addresses       : 0
Last Source Address        : 0000.0000.0000
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    0001.0001.0001    SecureDynamic       Fa0/1      15 (I)
   1    0001.0001.0002    SecureDynamic       Fa0/1      15 (I)
   1    0001.0001.1111    SecureConfigured    Fa0/1      16 (I)
   1    0001.0001.1112    SecureConfigured    Fa0/1      -
   1    0001.0001.1113    SecureConfigured    Fa0/1      -
   1    0005.0005.0001    SecureConfigured    Fa0/5      23
   1    0005.0005.0002    SecureConfigured    Fa0/5      23
   1    0005.0005.0003    SecureConfigured    Fa0/5      23
   1    0011.0011.0001    SecureConfigured    Fa0/11     25 (I)
   1    0011.0011.0002    SecureConfigured    Fa0/11     25 (I)
------------------------------------------------------------------------
Total Addresses in System :10
Max Addresses limit in System :6176
```

This is an example of output from the **show port-security interface fastethernet0/2 vlan** command:

```
Switch# show port-security interface fastethernet0/2 vlan
Default maximum: not set, using 6176
VLAN  Maximum    Current
    1    default          0
    5          5          0
```

This is an example of output from the **show port-security interface fastethernet0/5 address** command:

```
Switch# show port-security interface fastethernet0/5 address
Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0005.0005.0001    SecureConfigured    Fa0/5       19 (I)
   1    0005.0005.0002    SecureConfigured    Fa0/5       19 (I)
   1    0005.0005.0003    SecureConfigured    Fa0/5       19 (I)
------------------------------------------------------------------------
Total Addresses:3
```

Related Commands

Command	Description
switchport port-security	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

Use the **show power inline** user EXEC command to display the power status for the specified Power over Ethernet (PoE) port or for all PoE ports on the Catalyst 3550-24PWR switch.

show power inline [*interface-id*] **|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the interface.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.
12.1(19)EA1	The Class field was added to the output.
12.2(25)SE	The Max field was added to the output.

Usage Guidelines

This command is supported only on PoE-capable ports. PoE ports were previously referred to as inline power ports in earlier versions of the command reference.

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

Examples

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

```
Switch> show power inline
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
Fa0/2     auto   off        0.0     n/a                 n/a   15.4
Fa0/3     auto   on         5.4     Cisco IP phone 7960 n/a   15.4
Fa0/4     auto   on         15.4    Ieee PD                   15.4
Fa0/5     auto   off        0.0     n/a                 n/a   15.4
Fa0/6     auto   off        0.0     n/a                 n/a   15.4
Fa0/7     auto   off        0.0     n/a                 n/a   15.4
Fa0/8     auto   off        0.0     n/a                 n/a   15.4
Fa0/9     auto   off        0.0     n/a                 n/a   15.4
Fa0/10    auto   off        0.0     n/a                 n/a   15.4

<output truncated>
```

Table 2-24 show power inline Command Output Fields

Field	Description
Interface	Interface ID.
Admin	Administrative mode: auto or off.
Oper	Operating mode: • on—the powered device is detected and power is applied. • off—no power is applied. • faulty—device detection or a powered device is in a faulty state. • power-deny—a powered device is detected but no power is available.
Power	The supplied power in watts. A Cisco device shows reported power; a non-Cisco device is shown as an IEEE powered device at 15.4 W.
Device	The device type detected: n/a, unknown, Cisco PD, IEEE PD, <name from CDP>.
Class	The IEEE classification: n/a, Class <0-4>.
Max	The maximum power supported (15.4 W).

Related Commands

Command	Description
power inline	Enables or disables the PoE ports.

show running-config vlan

Use the **show running-config vlan** privileged EXEC command to display all or a range of VLAN-related configurations on the switch.

show running-config vlan [*vlan-ids*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-ids	(Optional) Display configuration information for a single VLAN identified by VLAN ID number or a range of VLANs separated by a hyphen. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show running-config vlan** command:

```
Switch# show running-config vlan 900-2005
Building configuration...

Current configuration:
!
vlan 907
!
vlan 920
!
vlan 1025
!
vlan 2000
!
vlan 2001
end
```

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
vlan (global configuration)	Enters config-vlan mode for creating and editing VLANs. When VLAN Trunking Protocol (VTP) mode is transparent, you can use this mode to create extended-range VLANs (VLAN IDs greater than 1005).
vlan database	Enters VLAN configuration mode for creating and editing normal-range VLANs.

show sdm prefer

Use the **show sdm prefer** privileged EXEC command to display information about the templates that can be used to maximize system resources for a particular feature, or use the command without a keyword to display the template in use.

show sdm prefer [**access** [**extended-match**] | **default** [**extended-match**] | **routing** [**extended-match**] | **vlan**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access	(Optional) Display the template that maximizes system resources for quality of service (QoS) classification and security access control entries (ACEs).
default	(Optional) Display the template that balances system resources among features.
extended-match	(Optional) Display the extended-match version of the indicated template that enables the switch to support 144-bit Layer 3 TCAM.
routing	(Optional) Display the template that maximizes system resources for routing.
vlan	(Optional) Display the template that maximizes system resources for Layer 2 VLANs.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(11)EA1	The **extended-match** keyword was added.

Usage Guidelines

If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your switch had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

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

Examples

This is an example of output from the **show sdm prefer** command on a Gigabit Ethernet switch, displaying the template currently in use:

```
Switch# show sdm prefer
The current template is default template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 16 routed interfaces and 1K VLANs.

 number of unicast mac addresses:  6K
 number of igmp groups:            6K
 number of qos aces:               2K
 number of security aces:          2K
 number of unicast routes:         12K
 number of multicast routes:       6K
```

This is an example of output from the **show sdm prefer** command on a Gigabit Ethernet switch when the default template has the **extended-match** keyword applied for 144-bit Layer 3 TCAM support:

```
Switch# show sdm prefer
The current template is the default extended-match template
 The selected template optimizes the resources in
 the switch to support this level of features for
 16 routed interfaces and 1K VLANs.

 number of unicast mac addresses:   6K
 number of igmp groups:             6K
 number of qos aces:                2K
 number of security aces:           2K
 number of unicast routes:          6K
 number of multicast routes:        6K
```

This is an example of output from the **show sdm prefer access** command on a Gigabit Ethernet switch, displaying the access template characteristics:

```
Switch# show sdm prefer access
access template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 16 routed interfaces and 1K VLANs.

 number of unicast mac addresses:  2K
 number of igmp groups:            8K
 number of qos aces:               2K
 number of security aces:          4K
 number of unicast routes:         4K
 number of multicast routes:       8K
```

Related Commands

Command	Description
sdm prefer	Sets the SDM template to maximize feature resource utilization for QoS classification and security ACEs, routing, or VLANs, or to the default template, or to reformat memory space to support 144-bit Layer 3 TCAM.

show setup express

Use the **show setup express** privileged EXEC command to show 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

Release	Modification
12.1(14)EA1	This command was introduced.

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
setup express	Enables Express Setup mode on the switch.

show spanning-tree

Use the **show spanning-tree** user EXEC command 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*] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree vlan *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree mst [**configuration** [**digest**] | *instance-id*] [**detail** | **interface** *interface-id* [**detail**]]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

bridge-group	(Optional) Specify the bridge group number. The range is 1 to 255.
active [**detail**]	(Optional) Display spanning-tree information only on active interfaces (only available in privileged EXEC mode).
backbonefast	(Optional) Display spanning-tree BackboneFast status.
blockedports	(Optional) Display blocked port information (only available in privileged EXEC mode).
bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display status and configuration of this switch (optional keywords only available in privileged EXEC mode).
detail [**active**]	(Optional) Display a detailed summary of interface information (**active** keyword only available in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (only available in privileged EXEC mode).

interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**]	(Optional) Display spanning-tree information for the specified interface (all options except **portfast** and **state** only available 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 64.
mst [**configuration** | [**digest]** *instance-id*] [**detail** | **interface** *interface-id* [**detail**]]	(Optional) Display the multiple spanning-tree (MST) region configuration and status (all options only available in privileged EXEC mode). • **digest**—(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). The terminology was updated for the implementation of the IEEE standard, and the *txholdcoun*t field was added. The new master role appears for boundary ports. The word *pre-standard* or *Pre-STD* appears when an IEEE standard bridge sends prestandard BPDUs on a port. The word *pre-standard (config)* or *Pre-STD-Cf* appears when a port has been configured to transmit prestandard BPDUs and no prestandard BPDU has been received on that port. The word *pre-standard (rcvd)* or *Pre-STD-Rx* appears when a prestandard BPDU has been received on a port that has not been configured to transmit prestandard BPDUs. A *dispute* flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated. • *instance-id*—You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of configured instances. • **interface** *interface-id*—(Optional) Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48. • **detail**—(Optional) Display detailed information for the instance or interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 64.
pathcost method	(Optional) Display the default path cost method (only available in privileged EXEC mode).
root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]	(Optional) Display root switch status and configuration (all keywords only available in privileged EXEC mode).
summary [**totals**]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section. The words *IEEE Standard* identify the MST version running on a switch.

uplinkfast	(Optional) Display spanning-tree UplinkFast status.
vlan *vlan-id* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display spanning-tree information for the specified VLAN (some keywords only available in privileged EXEC mode). The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC; indicated keywords available only in privileged EXEC mode

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **mst** keyword and options were added. The **brief** keyword was removed, and the **detail** keyword was added.
12.2(25)SEC	The **digest** keyword was added, and new digest and transmit hold count fields appear.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

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

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    20481
             Address     0008.217a.5800
             Cost        38
             Port        1 (GigabitEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0008.205e.6600
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 19        128.1    P2p
```

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 32768, sysid 1, address 0008.205e.6600
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 20481, address 0008.217a.5800
  Root port is 1 (GigabitEthernet0/1), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 3w0d 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

 Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.1.
   Designated root has priority 20481, address 0008.217a.5800
   Designated bridge has priority 65535, address 0050.2aed.5c80
   Designated port id is 128.26, designated path cost 19
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 947349

<output truncated>
```

This is an example of output from the **show spanning-tree interface fastethernet0/1** command:

```
Switch> show spanning-tree interface fastethernet0/1

Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 19        128.1    P2p
```

This is an example of output from the **show spanning-tree summary** command:

```
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 disabled
BackboneFast         is disabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          1          1
---------------------- -------- --------- -------- ---------- ----------
1 vlan                       0         0        0          1          1

<output truncated>
```

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         101-4094
1         1-100
-------------------------------------------------------------------------------
```

This is an example of output from the **show spanning-tree mst interface fastethernet0/1** command:

```
Switch# show spanning-tree mst interface fastethernet0/1

FastEthernet0/1 of MST00 is designated forwarding
Edge port:no             (default)        port guard :none        (default)
Link type:point-to-point (auto)           bpdu filter:disable     (default)
Boundary :internal                        bpdu guard :disable     (default)
Bpdus sent 84122, received 83933

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- --------------------------------
0        Desg FWD 200000    128.1    101-4094
1        Root FWD 200000    128.1    1-100
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped:  101-4094
Bridge      address 0005.7428.1f40  priority  32768 (32768 sysid 0)
Root        address 0001.42e2.cdc6  priority  32768 (32768 sysid 0)
            port    Gi0/2           path cost 200038
IST master  this switch
Operational hello time 2, forward delay 15, max age 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 200000    128.1    P2p
Gi0/2            Root FWD 200000    128.2    P2p Bound(PVST)
Gi0/5            Desg FWD 200000    128.5    P2p
```

Related Commands

Command	Description
clear spanning-tree counters	Clears the spanning-tree counters.
clear spanning-tree detected-protocols	Restarts the protocol migration process.
spanning-tree backbonefast	Enables the BackboneFast feature.
spanning-tree bpdufilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for a port is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show storm-control

Use the **show storm-control** user EXEC command to display broadcast, multicast, or unicast storm-control settings on the switch or on the specified interface.

show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Interface ID for the physical port.
broadcast	(Optional) Display broadcast storm information.
multicast	(Optional) Display multicast storm information.
unicast	(Optional) Display unicast storm information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

When you enter an *interface-id*, the storm-control thresholds appear for the specified interface.

If you omit the *interface-id* and specify a traffic type, settings appear for the specified traffic type for all ports on the switch.

If you do not enter a traffic type, settings appear for broadcast storm control.

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

Examples

This is an example of output from the **show storm-control** command. Because no traffic type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control
Interface  Filter State   Upper       Lower      Current
---------  -------------  ----------  ---------  ---------
Fa0/1      Forwarding     20 pps      10 pps     5 pps
Fa0/2      Forwarding     50.00%      40.00%     0.00%
<output truncated>
```

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> show storm-control fastethernet0/1
Interface  Filter State   Upper       Lower      Current
---------  -------------  ----------  ---------  ---------
Fa0/1      Forwarding     20 pps      10 pps     5 pps
```

Table 2-25 describes the fields in the **show storm-control** display.

Table 2-25 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking—Storm control is enabled, and a storm has occurred. • Forwarding—Storm control is enabled, and no storms have occurred. • Inactive—Storm control is disabled.
Upper	Displays the rising suppression level as a percentage of total available bandwidth or in packets per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth or in packets per second.
Current	Displays the bandwidth utilization of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth or in packets per second. If storm control is disabled, this field displays *N/A* (not applicable).

Related Commands

Command	Description
storm-control	Configures the broadcast, the multicast, or the unicast storm control with the specified suppression level.

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 [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If you have used the **system mtu** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

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

Examples

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

```
Switch# show system mtu
System MTU size is 1500 bytes
```

Related Commands

Command	Description
system mtu	Sets the maximum transmission unit (MTU) size for the switch.

show tcam

Use the **show tcam** user EXEC command to display information about the input security access control list (ACL) and output security ACL regions of the ternary content addressable memory (TCAM). Use the keywords to display information for a specific TCAM ID or specific characteristics.

show tcam {**inacl** | **outacl**} *tcam-id* {{**entries** [*entry-id*]} | {**masks** [*mask-id*]} | {**port-labels** [*label-id*]} | **size** |{**statistics** [**entries** | **hits** | **labels** | **masks**]} | {**vlan-labels** [*label-id*]}}[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

inacl	Display information about the input security ACL TCAM portion.
outacl	Display information about the output security ACL TCAM portion.
tcam-id	(Optional) Display information for a specific TCAM ID. The ID range varies from 1 to 3, depending on the switch model.
entries [*entry-id*]	Display one or all TCAM ACL entries and associated information. When all entries appear, the mask information also appears. This display output is a raw hex dump of information, intended for a Cisco technical support representative. The range is 0 to 65535.
masks [*mask-id*]	Display mask information. This display output is a raw hex dump of information, intended for a Cisco technical support representative. The range is 0 to 65535.
port-labels [*label-id*]	Display entries and associated information for a feature manager port label (see the **show fm** command). Port labels are used for port ACLs. This display output is a raw hex dump of information, intended for a Cisco technical support representative. The range is 0 to 127.
size	Display the total size of the regions of TCAM in which the ACLs are entered.
statistics [**entries** | **hits** | **labels** | **masks**]	Display allocation statistics for the input or output ACL TCAM region, including allocated and available masks and entries. (Optional) Display allocation statistics for entries, hits, labels, or masks. The **labels** keyword returns a total count of all labels present in TCAM.
vlan-labels [*label-id*]	Display entries and associated information for a feature manager VLAN label (see the **show fm** command). VLAN labels are used for router ACLs and VLAN maps. This display output is a raw hex dump of information, intended for a Cisco technical support representative. The range is 0 to 255.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **labels** [*label-id*] keywords were replaced by **port-labels** [*label-id*] and **vlan-labels** [*label-id*]

Usage Guidelines

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

These displays provide information that might be useful for Cisco technical support representatives troubleshooting the switch.

Examples

This is an example of output from the **show tcam inacl entries** command for TCAM 1:

```
Switch> show tcam inacl 1 entries
Label Value: 8192(vlan label 0) Number of entries: 12
Ts - timestamp, Tb - TableId, L - L4OpSelect (IP) or lsapValid (MAC)
M - IP (1) or MAC (0), R - routerMacAddress
I - ipOption, S - lookupSize, Pl - Port Label, Vl - VLAN Label
F - fragmentInfo (IP) or IP header checksum error (MAC)
D - DSCP (IP) or IP header error (MAC)
T - tcpPacket (IP) or cos (MAC)
U - udpPacket (IP) or reserved bits (MAC)
MapR - l4MapResult (IP TCP/UDP) or l3 protocol type (MAC)
S-addr - source address, D-addr - destination address
S-pr - l4 source port (IP TCP/UDP) or IP protocol number
D-pr - l4 destination port or version and type (IP IGMP)
or type and code (IP ICMP)
Index Ts Tb L M R I S Pl Vl F D  T U MapR S-addr   S-pr D-addr   D-pr As data
================================================================================
4     msk F 0 1 0 0 1 00 FF 0 00 1 1 0000 00000000 00FF E0000000 0000
32    1   9 0 1 0 0 1 00 00 0 00 0 0 0000 00000000 0009 E0000000 0000 00260086
5     msk F 0 1 0 1 1 00 FF 2 00 1 1 0000 00000000 0000 E0000000 FFFF
33    4   9 0 1 0 0 1 00 00 0 00 0 1 0000 00000000 0000 E0000000 0208 00260086
6     msk F 0 1 1 0 1 00 FF 0 00 1 1 0000 00000000 00FE 00000000 0000
48    42  9 0 1 1 0 1 00 00 0 00 0 0 0000 00000000 0058 00000000 0000 00260086
7     msk F 0 1 1 0 1 00 FF 0 00 1 1 0000 00000000 00FF 00000000 0000
49    4   9 0 1 1 0 1 00 00 0 00 0 0 0000 00000000 0009 00000000 0000 00260086
7     msk F 0 1 1 0 1 00 FF 0 00 1 1 0000 00000000 00FF 00000000 0000
51    64  9 0 1 1 0 1 00 00 0 00 0 0 0000 00000000 0067 00000000 0000 00260086
8     msk F 0 1 1 1 1 00 FF 2 00 1 1 0000 00000000 FFFF 00000000 0000
64    1   9 0 1 1 0 1 00 00 0 00 1 0 0000 00000000 0001 00000000 0000 00260086
9     msk F 0 1 1 1 1 00 FF 2 00 1 1 0000 00000000 0000 00000000 FFFF
65    4   9 0 1 1 0 1 00 00 0 00 1 0 0000 00000000 0000 00000000 00B3 00260086
9     msk F 0 1 1 1 1 00 FF 2 00 1 1 0000 00000000 0000 00000000 FFFF
67    64  9 0 1 1 0 1 00 00 0 00 0 1 0000 00000000 0000 00000000 0208 00260086
10    msk F 1 1 0 0 1 00 FF 0 00 0 0 FFFF 000000000000  010000000000
80    44  9 0 0 0 0 1 00 00 0 00 0 0 0806 000000000000  010000000000  00260086
11    msk F 1 1 1 0 1 00 FF 0 00 0 0 FFFF 000000000000  000000000000
81    42  9 0 0 1 0 1 00 00 0 00 0 0 0806 000000000000  000000000000  00260086
IP default entry
204   msk F 0 1 0 0 1 00 FF 0 00 0 0 0000 00000000 0000 00000000 0000
1636  42  9 0 1 0 0 1 00 00 0 00 0 0 0000 00000000 0000 00000000 0000 00000082
non-IP default entry
205   msk F 0 1 0 0 1 00 FF 0 00 0 0 0000 000000000000  000000000000
1637  48  9 0 0 0 0 1 00 00 0 00 0 0 0000 000000000000  000000000000  00000082
```

This is an example of output from the **show tcam outacl masks** command for TCAM 1:

```
Switch> show tcam outacl 1 masks
Number of active masks : 6
Mask Index : 0
F0 00 00 00 00 00 00 00 80 FF 00 00 00 00 00 00 00
Mask Index : 1
F0 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00
Mask Index : 508
F4 00 00 00 00 00 00 00 80 FF 00 00 00 00 00 00 00
Mask Index : 509
F4 00 00 00 00 00 00 00 80 FF 00 00 00 00 00 00 00
Mask Index : 510
F0 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
Mask Index : 511
F0 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
```

This is an example of output from the **show tcam inacl size** command for TCAM 1:

```
Switch# show tcam inacl 1 size
Ingress ACL TCAM Size:6592 Entries
```

This is an example of output from the **show tcam inacl statistics** command for TCAM 1:

```
Switch# show tcam inacl 1 statistics
Ingress ACL TCAM#1:Number of active labels:3
Ingress ACL TCAM#1:Number of masks   allocated:  14, available: 810
Ingress ACL TCAM#1:Number of entries allocated:  17, available:6575
```

Related Commands

Command	Description
show fm interface	Displays per-interface feature-manager information. Used with the **show fm label** command to show which features were able to fit into the hardware.
show fm	Displays feature-manager information for a specified label to list features associated with the label that were not able to fit into hardware.

show tcam pbr

Use the **show tcam pbr** user EXEC command to display the policy-based routing (PBR) region of the specified ternary content addressable memory (TCAM). Use the keywords to display information for a specific TCAM ID or specific characteristics.

show tcam pbr *tcam-id* {{**entries** [*entry-id*]} | {**port-labels** [*label-id*]} | {**vlan-labels** [*label-id*]} | {**masks** [*mask-id*]} | **size** | {**statistics** [**entries** | **hits** | **labels** | **masks**]}} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

tcam-id	Identify the TCAM ID for displaying PBR TCAM information.
entries [*entry-id*]	Display one or all TCAM PBR entries and associated information. When all entries appear, the mask information also appears. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 65535.
port-labels [*label-id*]	Display entries and associated information for a port label. **Note** Though visible in the command-line help string, the **port-labels** keyword is not supported for PBR.
vlan-labels [*label-id*]	Display entries and associated information for a PBR VLAN label. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 255.
masks [*mask-id*]	Display mask information. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 65535.
size	Display the size of the PBR TCAM region.
statistics [**entries** | **hits** | **labels** | **masks**]	Display allocation statistics for the PBR TCAM region, including allocated and available masks and entries. (Optional) Display allocation statistics for entries, hits, labels, or masks. The **labels** keyword returns a total count of all labels present in TCAM.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(13)EA1	This command was introduced.

Usage Guidelines

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

You can use the **show tcam pbr** *tcam-id* **entries** [*entry-id*] command to display all PBR entries. You can use the **show tcam pbr** *tcam-id* **vlan-labels** [*label-id*] command to display per-VLAN TCAM entries with the policy label. You can use the **show fm interface** *interface-id* command to display the policy label for the interface on which PBR is enabled.

These displays provide information that might be useful for Cisco technical support representatives troubleshooting the switch.

Examples

This is an example of output from the **show tcam pbr masks** command for TCAM 1:

```
Switch> show tcam pbr 1 masks
Number of active masks : 2
Mask Index : 0
F1 FF FF FF FF 00 00 00 00 80 FF 00 00 00 00 00 00 00
Mask Index : 1
F1 FF FF FF 00 FF FF FF 00 80 FF 00 00 00 00 00 00 00
```

This is an example of output from the **show tcam pbr entries** command for TCAM 1:

```
Switch> show tcam pbr 1 entries
00:07:11: %SYS-5-CONFIG_I: Configured from console by console
Number of active labels: 1

Label Value :       8201(vlan label 9)
Number of entries : 2
Entry List
----------
Mask Index : 0
F1 FF FF FF FF 00 00 00 00 80 FF 00 00 00 00 00 00 00
Entry Index : 0  Timestamp: 1
C0 0A 01 01 02 00 00 00 00 80 09 00 00 00 00 00 00 00 As Data(hex) : 00078006
Mask Index : 1
F1 FF FF FF 00 FF FF FF 00 80 FF 00 00 00 00 00 00 00
Entry Index : 1  Timestamp: 4
C0 0A 01 02 00 0A 04 05 00 80 09 00 00 00 00 00 00 00 As Data(hex) : 00048000
```

This is an example of output from the **show tcam pbr statistics** command for TCAM 1:

```
Switch> show tcam pbr 1 statistics
PBR TCAM#1: Number of active labels: 1
PBR TCAM#1: Number of masks   allocated:    2
PBR TCAM#1: Number of entries allocated:    2
```

This is an example of output from the **show tcam pbr vlan-label** command for TCAM 1:

```
Switch> show tcam pbr 1 vlan-label 9
Label Value :       8201(vlan label 9)
Number of entries : 2
Entry List
----------
Mask Index : 0
F1 FF FF FF FF 00 00 00 00 80 FF 00 00 00 00 00 00 00
Entry Index : 0  Timestamp: 1
C0 0A 01 01 02 00 00 00 00 80 09 00 00 00 00 00 00 00 As Data(hex) : 00078006
Mask Index : 1
F1 FF FF FF 00 FF FF FF 00 80 FF 00 00 00 00 00 00 00
Entry Index : 1  Timestamp: 4
C0 0A 01 02 00 0A 04 05 00 80 09 00 00 00 00 00 00 00 As Data(hex) : 00048000
```

show tcam qos

Use the **show tcam qos** user EXEC command to display about the quality of service (QoS) region of the specified ternary content addressable memory (TCAM). Use the keywords to display information for a specific TCAM ID or specific characteristics.

show tcam qos *tcam-id* {{**entries** [*entry-id*]} | {**port-labels** [*label-id*]} | {**vlan-labels** [*label-id*]} | {**masks** [*mask-id*]} | **size** | {**statistics** [**entries** | **hits** | **labels** | **masks**]}} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

tcam-id	Identify the TCAM ID for displaying QoS TCAM information. (Optional) Display information for a specific TCAM ID. The ID range varies from 1 to 3, depending on the switch model.
entries [*entry-id*]	Display one or all TCAM QoS entries and associated information. When all entries appear, the mask information also appears. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 65535.
port-labels [*label-id*]	Display entries and associated information for a QoS port label. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 255.
vlan-labels [*label-id*]	Display entries and associated information for a QoS VLAN label. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 255.
masks [*mask-id*]	Display mask information. This display output is a raw hex dump of information intended for a Cisco technical support representative. The range is 0 to 65535.
size	Display the size of the QoS TCAM region.
statistics [**entries** | **hits** | **labels** | **masks**]	Display allocation statistics for the QoS TCAM region, including allocated and available masks and entries. (Optional) Display allocation statistics for entries, hits, labels, or masks. The **labels** keyword returns a total count of all labels present in TCAM.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **labels** [*label-id*] keywords were replaced by **port-labels** [*label-id*] and **vlan-labels** [*label-id*].

Usage Guidelines

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

You can use the **show tcam qos** *tcam-id* **entries** [*entry-id*] command to display all QoS entries including per-port per-VLAN QoS information. You also can use the **show tcam qos** *tcam-id* **port-labels** [*label-id*] **vlan-labels** [*label-id*] command to display per-port per-VLAN TCAM entries with both the port label and the VLAN label.

These displays provide information that might be useful for Cisco technical support representatives troubleshooting the switch.

Examples

This is an example of output from the **show tcam qos masks** command for TCAM 2:

```
Switch> show tcam qos 2 masks
Number of active masks : 4
Mask Index : 252
F4 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00
Mask Index : 253
F4 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00
Mask Index : 254
F0 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
Mask Index : 255
F0 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00
```

This is an example of output from the **show tcam qos entries** command for TCAM 1:

```
Switch> show tcam qos 1 entries
No active labels/entries
```

This is an example of output from the **show tcam qos statistics** command for TCAM 1:

```
Switch> show tcam qos 1 statistics
QoS TCAM#1: Number of active labels: 0
QoS TCAM#1: Number of masks   allocated:    4, available:  412
QoS TCAM#1: Number of entries allocated:    1, available: 3327
```

show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

show udld [*interface-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces appear.

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

Examples

This is an example of output from the **show udld gigabitethernet0/1** command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-26 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: Gi0/2
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/1
    Message interval: 5
    CDP Device name: Switch-A
```

Table 2-26 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.
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).

This is an example of output from the **show udld** interface configuration command when the aggressive mode is configured:

```
Switch# show udld gigabitethernet0/1
Interface Gi0/1
---
Port enable administrative configuration setting:Enabled / in aggressive mode
Port enable operational state:Enabled / in aggressive mode
Current bidirectional state:Unknown
Current operational state:Link down
Message interval:7
Time out interval:5
No neighbor cache information stored
```

Related Commands

Command	Description
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

show version

Use the **show version** user EXEC command to display version information for the hardware and firmware.

show version [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

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

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-IPSERVICES-M), Version 12.2(25)SEB, RELEASE SOFTWARE
VERSION
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Tue 15-FEB-05 07:06 by antonino
Image text-base: 0x00003000, data-base: 0x007175BC

ROM: Bootstrap program is C3550 boot loader

tslo-2 uptime is 4 days, 1 hour, 6 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipservices-mz.122-25.SEB"

cisco WS-C3550-12T (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image
Target IOS Version 12.2(25)SEB
```

```
Ethernet-controller 1 has 1 Gigabit Ethernet/IEEE 802.3 interface<output truncated>

The password-recovery mechanism is enabled.
384K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:02:4B:29:2B:00
Configuration register is 0x10F
```

show vlan

Use the **show vlan** user EXEC command 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** | **dot1q tag native** | **id** *vlan-id* | **internal usage** | **name** *vlan-name* | **remote-span** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Display one line for each VLAN with the VLAN name, status, and its ports.
dot1q tag native	(Optional) Display the IEEE 802.1Q native VLAN tagging status.
id *vlan-id*	(Optional) Display information about a single VLAN identified by VLAN ID number or a range of VLANs. The range is 1 to 4094.
internal usage	(Optional) Display list of VLANs being used internally by the switch. These VLANs are always from the extended range (VLAN IDs 1006 to 4094), and you cannot create VLANs with these IDS by using the **vlan** global configuration command until you remove them from internal use.
name *vlan-name*	(Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Display information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Display VLAN summary information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **ifindex** and **private-vlan** keywords are not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **dot1q tag native**, **internal usage**, and **summary** keywords were added.
12.1(11)EA1	The **remote-span** keyword was added.
12.1(13)EA1	The value for **id** *vlan-id* was changed.

Usage Guidelines

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

Examples

This is an example of output from the **show vlan** command. Table 2-27 describes each field in the display.

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/5, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/11, Fa0/12
                                                Gi0/1, Gi0/2
2    VLAN0002                         active
51   VLAN0051                         active
52   VLAN0052                         active
100  VLAN0100                         suspended Fa0/3
400  VLAN0400                         suspended
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
51   enet  100051     1500  -      -      -        -    -        0      0
52   enet  100052     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
400  enet  100400     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   3276   -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ieee -        0      0
1005 trnet 101005     1500  -      -      15       ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Table 2-27 show vlan Command Output Fields

Field	Description
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.

Table 2-27 show vlan Command Output Fields (continued)

Field	Description
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.
AREHops	Maximum number of hops for All-Routes Explorer frames—possible values are 1 through 13; the default is 7.
STEHops	Maximum number of hops for Spanning-Tree Explorer frames—possible values are 1 through 13; the default is 7.
Backup CRF	Status of whether or not the Token Ring concentrator relay function (TrCRF) is a backup path for traffic.
Remote SPAN VLANs	Identify any RSPAN VLANs that have been configured.

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

```
Switch> show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

This is an example of output from the **show vlan id** command. The specified VLAN is in the extended VLAN range.

```
Switch# show vlan id 2005

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2005 VLAN2005                         active    Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2005 enet  102005     1500  -      -      -        -    -        0      0
```

This is an example of output from the **show vlan dot1q tag native** command:

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

This is an example of output from the **show vlan internal usage** command. It shows that VLANs 1025 and 1026 are being used as internal VLANs for Fast Ethernet routed ports 23 and 24. If you want to use one of these VLAN IDs, you must first shut down the routed port, which releases the internal VLAN, and then create the extended-range VLAN. When you start up the routed port, another internal VLAN number is assigned to it.

```
Switch> show vlan internal usage

VLAN Usage
---- -------------
1025 FastEthernet0/23
1026 FastEthernet0/24
```

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

```
Switch> show vlan summary
Number of existing VLANs           : 7
 Number of existing VTP VLANs      : 7
 Number of existing extended VLANs : 0
```

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.
vlan (global configuration)	Enables config-vlan mode where you can configure VLANs 1 to 4094.
vlan (VLAN configuration)	Configures VLAN characteristics in the VLAN database. Only available for normal-range VLANs (VLAN IDs 1 to 1005).

show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or all VLAN access maps.

show vlan access-map [*mapname*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

mapname	(Optional) Name of a specific VLAN access map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show vlan access-map** command:

```
Switch# show vlan access-map
Vlan access-map "map_1" 10
  Match clauses:
     ip address: ip1
  Action:
     drop
Vlan access-map "map_1" 20
  Match clauses:
     mac address: mac1
  Action:
     forward
Vlan access-map "map_1" 30
  Match clauses:
  Action:
     drop
```

Related Commands

Command	Description
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan filter

Use the **show vlan filter** privileged EXEC command to display information about all VLAN filters or about a particular VLAN or VLAN access map.

show vlan filter [**access-map** *name* | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access-map *name*	(Optional) Display filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Display filtering information for the specified VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

show vmps

Use the **show vmps** user EXEC command 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 vmps [**statistics**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

statistics	(Optional) Display VQP client-side statistics and counters.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

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

```
Switch> show vmps
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 vmps statistics** command. Table 2-28 describes each field in the display.

```
Switch> show vmps 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 2-28 show vmps 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.
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

Command	Description
clear vmps statistics	Clears the statistics maintained by the VQP client.
vmps reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.
vmps retry	Configures the per-server retry count for the VQP client.
vmps server	Configures the primary VMPS and up to three secondary servers.

show vtp

Use the **show vtp** user EXEC command to display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters.

show vtp {**counters** | **status**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

counters	Display the VTP statistics for the switch.
status	Display general information about the VTP management domain status.
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.
| **include**	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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

Examples

This is an example of output from the **show vtp counters** command. Table 2-29 describes each field in the display.

```
Switch> show vtp counters

VTP statistics:
Summary advertisements received    : 38
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 13
Subset advertisements transmitted  : 3
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
---------------- ---------------- ---------------- ---------------------------
Fa0/9               827              824              0
Fa0/10              827              823              0
Fa0/11              827              823              0
```

Table 2-29 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.
Number of configuration revision errors	Number of revision errors. 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. 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. These errors means that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of configuration digest errors	Number of MD5 digest errors. 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. These errors mean that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of version 1 errors. 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.
Join Transmitted	Number of VTP pruning messages sent on the trunk.

Table 2-29 show vtp counters Field Descriptions (continued)

Field	Description
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. Table 2-30 describes each field in the display.

```
Switch> show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.20.135.196 on interface Vl1 (lowest numbered VLAN interface found)
```

Table 2-30 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	Displays the VTP operating mode, which can be server, client, or transparent. 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. **Note** The switch automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM; it cannot return to server mode until the NVRAM is functioning. Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough NVRAM 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. 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

Table 2-30 show vtp status Field Descriptions (continued)

Field	Description
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.

Related Commands

Command	Description
clear vtp counters	Clears the VTP and pruning counters.
vtp (global configuration)	Configures the VTP filename, interface name, domain name, and mode.
vtp (privileged EXEC)	Configures the VTP password, pruning, and version.
vtp (VLAN configuration)	Configures the VTP domain name, password, pruning, and mode.

shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled port or a switch virtual interface (SVI).

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **shutdown** command for a port causes it 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 an interface:

```
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
show interfaces	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*

Syntax Description

vlan-id	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.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **shutdown vlan** command does not change the VLAN information in the VTP database. It shuts down traffic locally, but the switch still advertises VTP information.

Examples

This example shows how to shutdown traffic on VLAN 2:

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

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

Related Commands

Command	Description
shutdown (config-vlan mode)	Shuts down local traffic on the VLAN when in config-VLAN mode (accessed by the **vlan** *vlan-id* global configuration command).
vlan database	Enters VLAN configuration mode.

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 [**bgp** | **bridge** | **cluster** | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature** | **voltage**] | **flash** | **hsrp** | **ipmulticast** | **mac-notification** | **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*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

no snmp-server enable traps [**bgp** | **bridge** | **cluster** | **config** | **copy-config** | **entity** | **envmon** | **flash** | **hsrp** | **ipmulticast** | **mac-notification** | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim [invalid-pim-message | neighbor-change | rp-mapping-change]** | **port-security** | **rtr** | **snmp** | **storm-control trap-rate** | **stpx** | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

Syntax Description

bgp	(Optional) Enable Border Gateway Protocol (BGP) state change traps. **Note** This keyword is available only when the enhanced multilayer image is installed.
bridge	(Optional) Enable Spanning Tree Protocol (STP) bridge MIB traps.
cluster	(Optional) Enable cluster traps.
config	(Optional) Enable SNMP configuration traps.
copy-config	(Optional) Enable SNMP copy-configuration traps.
entity	(Optional) Enable SNMP entity traps.
envmon [**fan** | **shutdown** | **status** | **supply** | **temperature** | **voltage**]	(Optional) Enable SNMP environmental traps. The keywords have these meanings: • **fan**—(Optional) Enable fan traps. • **shutdown**—(Optional) Enable environmental monitor shutdown traps. • **status**—(Optional) Enable environmental status-change traps. • **supply**—(Optional) Enable environmental monitor supply traps. • **temperature**—(Optional) Enable environmental monitor temperature traps. • **voltage**—(Optional) Enable environmental monitor voltage traps.
flash	(Optional) Enable SNMP FLASH notifications.
hsrp	(Optional) Enable Hot Standby Router Protocol (HSRP) traps.
ipmulticast	(Optional) Enable IP multicast routing traps.
mac-notification	(Optional) Enable MAC address notification traps.
msdp	(Optional) Enable Multicast Source Discovery Protocol (MSDP) traps.

ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]	(Optional) Enable Open Shortest Path First (OSPF) traps. The keywords have these meanings: • **cisco-specific**—(Optional) Enable Cisco-specific traps. • **errors**—(Optional) Enable error traps. • **lsa**—(Optional) Enable link-state advertisement (LSA) traps. • **rate-limit**—(Optional) Enable rate-limit traps. • **retransmit**—(Optional) Enable packet-retransmit traps. • **state-change**—(Optional) Enable state-change traps.
pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]	(Optional) Enable Protocol-Independent Multicast (PIM) traps. The keywords have these meanings: • **invalid-pim-message**—(Optional) Enable invalid PIM message traps. • **neighbor-change**—(Optional) Enable PIM neighbor-change traps. • **rp-mapping-change**—(Optional) Enable rendezvous point (RP)-mapping change traps.
port-security [**trap-rate** *value*]	(Optional) Enable port security traps. Use the **trap-rat**e keyword to set the number of traps per second. The range is 0 to 1000 seconds.
rtr	(Optional) Enable SNMP Response Time Reporter traps.
snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	(Optional) Enable SNMP traps. The keywords have these meanings: • **authentication**—(Optional) Enable authentication trap. • **coldstart**—(Optional) Enable cold start trap. • **linkdown**—(Optional) Enable linkdown trap. • **linkup**—(Optional) Enable linkup trap. • **warmstart**—(Optional) Enable warmstart trap.
storm-control trap-rate *value*	(Optional) Enable storm-control traps. Use the **trap-rat**e keyword to set the maximum number of storm-control 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).
stpx	(Optional) Enable SNMP STPX MIB traps.
syslog	(Optional) Enable SNMP syslog traps.
tty	(Optional) Send TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enable SNMP VLAN membership traps.
vlancreate	(Optional) Enable SNMP VLAN-created traps.
vlandelete	(Optional) Enable SNMP VLAN-deleted traps.
vtp	(Optional) Enable VLAN Trunking Protocol (VTP) traps.

Note Though visible in the command-line help strings, the **cpu** [**threshold**], **flash insertion**, and **flash removal** keywords are not supported. The **snmp-server enable informs** command is not supported. To enable sending of SNMP inform notifications, use the **snmp-server enable traps** command combined with the **snmp-server host** *host-addr* **informs** command.

Defaults

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	The **mac-notification** keyword was added.
12.1(9)EA1	The **vlan-membership** keyword was added.
12.1(11)EA1	The **bgp** keyword was added (enhanced multilayer image only).
12.1(12c)EA1	The **envmon [fan**| **shutdown** | **status** | **supply** | **temperature** | **voltage]** keywords were added.
12.1(13)EA1	The **port-security** and **trap-rate** keywords were added.
12.1(14)EA1	The **authentication**, **bridge**, **coldstart**, **copy-config**, **flash**, **linkdown**, **linkup**, **stpx**, **syslog**, **vlancreate**, **vlandelete**, and **warmstart** keywords were added.
12.2(25)SE	The **ipmulticast**, **msdp**, **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**], **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**], **storm-control trap-rate** *value*, and **tty** 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 trap types are sent.

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

Note Informs are not supported in SNMPv1.

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

Examples

This example shows how to 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
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2** > **File Management Commands** > **Configuration File Management Commands**.
snmp-server host	Specifies the host that receives SNMP traps.

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* [**udp-port** *port*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

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

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
udp-port *port*	(Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is 0 to 65535.
informs | **traps**	(Optional) Send SNMP traps or informs to this host.
version 1 | **2c** | **3**	(Optional) Version of the SNMP used to send the traps. These keywords are supported: **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. These optional keywords can follow the version 3 keyword: • **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth** | **noauth** | **priv**] keyword choice is not specified. • **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called *privacy*). **Note** The **priv** keyword is available only when the cryptographic (encrypted) software image is installed.
vrf *vrf-instance*	(Optional) Virtual private network (VPN) routing instance and name for this host.

community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command.
notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords: • **bgp**—Send Border Gateway Protocol (BGP) state change traps. This keyword is available only when the enhanced multilayer image is installed on the stack master. • **bridge**—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps. • **cluster**—Send cluster member status traps. • **config**—Send SNMP configuration traps. • **copy-config**—Send SNMP copy configuration traps. • **entity**— Send SNMP entity traps. • **envmon**—Send environmental monitor (EnvMon) traps. • **flash**—Send SNMP FLASH notifications. • **hsrp—**Send SNMP Hot Standby Router Protocol (HSRP) traps. • **ipmulticast—**Send SNMP IP multicast routing traps. • **mac-notification—**Send SNMP MAC notification traps. • **msdp—**Send SNMP Multicast Source Discovery Protocol (MSDP) traps. • **ospf—**Send Open Shortest Path First (OSPF) traps. • **pim—**Send SNMP Protocol-Independent Multicast (PIM) traps. • **port-security—**Send SNMP port-security traps. • **rtr—**Send SNMP Response Time Reporter traps. • **snmp—**Send SNMP-type traps. • **storm-control—**Send SNMP storm-control traps. • **stpx—**Send SNMP STP extended MIB traps. • **syslog—**Send SNMP syslog traps. • **tty—**Send TCP connection traps. • **vlan-membership—** Send SNMP VLAN membership traps. • **vlancreate—**Send SNMP VLAN-created traps. • **vlandelete—**Send SNMP VLAN-deleted traps. • **vtp—**Send SNMP VLAN Trunking Protocol (VTP) traps.

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

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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	The **mac-notification** keyword was added.
12.1(9)EA1	The **vlan-membership** keyword was added.
12.1(11)EA1	The version **3** option was added, with the **auth**, **noauth**, and **priv** keywords. The **bgp** keyword was added.
12.1(12c)EA1	The **envmon** keyword was added.
12.1(13)EA1	The **port-security** keyword was added.
12.1(14)EA1	The **bridge**, **copy-config**, **flash**, **stpx**, **syslog**, **vlancreate**, and **vlandelete** keywords were added.
12.2(25)SE	The **ipmulticast**, **msdp**, **ospf**, **pim**, **storm-control trap rate** *value*, and **vrf** *vrf-instance* 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

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2** > **File Management Commands** > **Configuration File Management Commands**.
snmp-server enable traps	Enables SNMP notification for various trap types or inform requests.

snmp-server ip

Use the **snmp-server ip** global configuration command to prioritize Simple Network Management Protocol (SNMP) notifications using either IP precedence or Differentiated Services Code Point (DSCP) marking. Use the **no** form of this command to return to the default setting.

snmp-server ip {**precedence** *new-precedence* | **dscp** *new-dscp*}

no snmp-server ip {**precedence** | **dscp**}

Syntax Description

precedence *new-precedence*	Assign a new IP precedence value to outgoing SNMP traffic. The range is 0 to 7.
dscp *new-dscp*	Assign a new DSCP value to outgoing SNMP traffic. The range is 0 to 63.

Defaults

The default marker is 0 (best effort).

Command Modes

Global configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.

Usage Guidelines

You can improve the delivery of SNMP trap notifications by assigning a higher IP precedence or DSCP marker to them. The default marker, 0, forwards SNMP packets as normal traffic. Markers with higher values invoke preferential forwarding that moves the packets through the network more efficiently, even during periods of congestion. The amount of preference increases with the marker value. The highest marker values, 7 for IP precedence and 63 for DSCP, are generally reserved for network control traffic. The marker value that you set with this command applies to all outgoing SNMP notifications.

DSCP has partial backward-compatibility with IP precedence. To use DSCP-like IP precedence, use the following DSCP values: 0, 8, 16, 24, 32, 40, 48, and 56.

Use the **snmp-server enable traps** command to allow traps or informs to be sent, when supported. Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command.

Examples

This example shows how to set the IP precedence to 5:

```
Switch(config)# snmp-server ip precedence 5
```

This example shows how to set the DSCP marking to 40:

```
Switch(config)# snmp-server ip dscp 40
```

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

Related Commands

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
snmp-server host	Specifies the host that receives SNMP traps.
snmp-server enable traps	Enables SNMP notification for various trap types or inform requests.

snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable the Simple Network Management Protocol (SNMP) MAC address 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 {**added** | **removed**}

no snmp trap mac-notification {**added** | **removed**}

Syntax Description

added	Enable the MAC notification trap whenever a MAC address is added on this interface.
removed	Enable the MAC notification trap whenever 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

Command History

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added to an interface:

```
Switch(config)# interface fastethernet0/4
Switch(config-if)# snmp trap mac-notification added
```

You can verify your settings by entering the **show mac address-table notification interface** privileged EXEC command.

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
mac address-table notification	Enables the MAC address notification feature.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.

spanning-tree backbonefast

Use the **spanning-tree backbonefast** global configuration command to enable the BackboneFast feature. Use the **no** form of this 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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You can configure 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 is started when a root port or blocked port on a switch receives inferior bridge protocol data units (BPDUs) from its designated bridge. An inferior BPDU identifies one switch as both the root bridge and the designated bridge. 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 bridge 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 ports 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
show spanning-tree summary	Displays a summary of the spanning-tree port states.

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command to prevent a port 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

Syntax Description

disable	Disable BPDU filtering on the specified interface.
enable	Enable BPDU filtering on the specified interface.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

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 ports 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.

When you configure Layer 2 protocol filtering, the spanning-tree BPDU filtering feature is automatically enabled on the port.

Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	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 a port 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

Syntax Description

disable	Disable BPDU guard on the specified interface.
enable	Enable BPDU guard on the specified interface.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent a port 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 ports 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.

Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	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**

Syntax Description

vlan *vlan-id*	(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.
cost	Path cost can range from 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 Mbps—4
- 100 Mbps—19
- 10 Mbps—100

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The range for the *cost* variable increased.
12.1(13)EA1	The value for the *vlan-id* variable was changed.

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.

Examples

This example shows how to set a path cost of 250 on an interface:

```
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost of 300 for VLAN 10:

```
Switch(config-if)# spanning-tree vlan 10 cost 300
```

This example shows how to set a path cost of 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

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	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 a loop that occurred because of 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

Release	Modification
12.1(13)EA1	This command was introduced.

Usage Guidelines

When the switch detects a loop that is caused by an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To determine which switch ports are in EtherChannel misconfiguration, 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 feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Related Commands

Command	Description
errdisable recovery cause channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disable state.
show etherchannel summary	Displays EtherChannel information for a channel as a one-line summary for each channel group.
show interfaces status err-disabled	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
12.1(8)EA1	This command was introduced.

Usage Guidelines

In Cisco IOS Release 12.1(8)EA1 and later, Catalyst 3550 switches support the IEEE 802.1t spanning-tree extensions, and 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 an instance identifier for the multiple spanning tree [MST]). In earlier releases, the switch priority is a 16-bit value.

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. With earlier releases, spanning tree used one MAC address per VLAN to make the bridge ID unique for each VLAN.

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 running older software.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of spanning-tree port states.
spanning-tree mst root	Configures the multiple spanning-tree (MST) root switch priority and timers based on the network diameter.
spanning-tree vlan priority	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

loop	Enable loop guard.
none	Disable root guard or loop guard.
root	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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **loop** keyword was added.

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 a port to be selected as the root port, the port 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 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 ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the port is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the port in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command.

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 interface:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified interface:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# spanning-tree guard loop
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree vlan priority	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 port, and to enable Rapid Spanning-Tree Protocol (RSTP) 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

Syntax Description

point-to-point	Specify that the link type of a port is point-to-point.
shared	Specify that the link type of a port is shared.

Defaults

The switch derives the link type of a port from the duplex mode. A full-duplex port is considered a point-to-point link, and a half-duplex port is considered a shared link.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

You can override the default setting of the link type by using the **spanning-tree link-type** command; for example, a half-duplex link can be physically connected point-to-point to a single port 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.

Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent RSTP rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays multiple spanning-tree (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

Release	Modification
12.1(9)EA1	This command was introduced.

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 ports only if the port is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the port in all MST instances.

Loop guard operates only on ports that are considered point-to-point by the spanning tree.

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
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified interface.

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

Syntax Description

mst	Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
pvst	Enable PVST+ (based on IEEE 802.1D).
rapid-pvst	Enable rapid PVST+ (based on IEEE 802.1w).

Defaults

The default mode is PVST+.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The **rapid-pvst** keyword was added.

Usage Guidelines

The switch must run all STP instances in one of these modes: PVST+, rapid PVST+, or MST. In other words, you cannot run STP in any two modes at the same time.

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 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
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

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

Syntax Description

This command has no arguments or keywords.

Defaults

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.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.2(25)SEC	The *instance-id* range changed to 1 to 4094.

Usage Guidelines

Entering 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 the 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.

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 VLAN 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

Command	Description
show spanning-tree mst configuration	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

instance-id	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.
cost	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 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The value for the *instance-id* variable was changed.
12.2(25)SEC	The *instance-id* range changed to1 to 4094.

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 an interface associated with instances 2 and 4:

```
Switch(config)# interface fastethernet0/1
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.

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	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 determines 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

Syntax Description

seconds	Length of the listening and learning states. The range is 4 to 30 seconds.

Defaults

The default is 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:

```
Switch(config)# spanning-tree mst forward-time 18
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

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

Syntax Description

seconds	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.

Defaults

The default is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* 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 **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree hello time to 3 seconds for all MST instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays multiple spanning-tree (MST) information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	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

Syntax Description

seconds	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.

Defaults

The default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* 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 **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst max-age** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree max-age to 30 seconds for all MST instances:

```
Switch(config)# spanning-tree mst max-age 30
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays multiple spanning-tree (MST) information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

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 a port 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

Syntax Description

hop-count	Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.

Defaults

The default is 20 hops.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.2(25)SEC	The *hop-count* range changed to 1 to 255.

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 port when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

Examples

This example shows how to set the spanning-tree max-hops to 10 for all MST instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays multiple spanning-tree (MST) information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

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 determine which 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**

Syntax Description

instance-id	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.
priority	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.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The values for the *instance-id* and the *priority* variables were changed.
12.2(25)SEC	The *instance-id* range changed to 1 to 4094.

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 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 instance 20 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree mst 20 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
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst priority	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

Release	Modification
12.2(25)SEC	This command was introduced.

Usage Guidelines

Even with this configuration, the port can accept both prestandard and standard BPDUs. In the case of a mismatch with the neighbor type, only the common and internal spanning tree (CIST) runs on this interface.

Note If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the s**panning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple Spanning-Tree Protocol (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighb ors, 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
show spanning-tree mst *instance-id*	Displays multiple spanning-tree (MST) information, including the *prestandard* flag, for the specified interface.

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**

Syntax Description

instance-id	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.
priority	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. 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.

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The value for the *instance-id* variable was changed.
12.2(25)SEC	The *instance-id* range changed to 1 to 4094.

Examples

This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instance (MST) 20:

```
Switch(config)# spanning-tree mst 20 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst port-priority	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 setting.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

instance-id	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.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(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.
hello-time *seconds*	(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

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The value for the *instance-id* variable was changed.
12.2(25)SEC	The *instance-id* range changed to 1 to 4094.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command used 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).

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

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	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 determine which 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**

Syntax Description

vlan *vlan-id*	(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.
priority	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.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(13)EA1	The values for the *vlan-id* and the *priority* variables were changed.

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. only on the range of VLANs specified by that command. On the VLANs that are not specified by the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command, the **spanning-tree port-priority** *priority* command takes effect.

Examples

This example shows how to increase the likelihood that the interface will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

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

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree vlan priority	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 ports, the BPDU guard feature on Port Fast-enabled ports, or the Port Fast feature on all nontrunking ports. The BPDU filtering feature prevents the switch port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled ports that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default setting.

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

Syntax Description

bpdufilter default	Globally enable BPDU filtering on Port Fast-enabled ports and prevent the switch port connected to end stations from sending or receiving BPDUs.
bpduguard default	Globally enable the BPDU guard feature on Port Fast-enabled ports and place the ports that receive BPDUs in an error-disabled state.
default	Globally enable the Port Fast feature on all nontrunking ports. When the Port Fast feature is enabled, the port 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 ports unless they are individually configured.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **bpdufilter default** and **default** keywords were added.

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 ports that are Port Fast-enabled (the ports are in a Port Fast-operational state). The ports 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 ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled port, the port 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 bdpufilter** 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.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port 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 bdpuguard** interface configuration command.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports 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 port 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 ports 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 ports:

```
Switch(config)# spanning-tree portfast default
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree bpdufilter	Prevents a port from sending or receiving BPDUs.
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	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

Syntax Description

disable	(Optional) Disable the Port Fast feature on the specified interface.
trunk	(Optional) Enable the Port Fast feature on a trunking interface.

Defaults

The Port Fast feature is disabled on all interfaces; however, it is automatically enabled on dynamic-access ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **disable** and **trunk** keywords were added.

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.

A port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting 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.

Examples

This example shows how to enable the Port Fast feature on an interface:

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# spanning-tree portfast
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree bpdufilter	Prevents a port from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts a port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.

spanning-tree stack-port

Use the **spanning-tree stack-port** interface configuration command to enable cross-stack UplinkFast (CSUF) on an interface and to accelerate the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself. Use the **no** form of this command to return to the default setting.

spanning-tree stack-port

no spanning-tree stack-port

Syntax Description

This command has no arguments or keywords.

Defaults

CSUF is disabled on all interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

This command is effective only if you enable the UplinkFast feature by using the **spanning-tree uplinkfast** global configuration command.

Use this command only on access switches.

The CSUF feature is supported only when the switch is running per-VLAN spanning-tree plus (PVST+). It is not supported when the switch is running rapid PVST+ or multiple spanning tree (MST).

You can enable CSUF only on one stack-port Gigabit Interface Converter (GBIC) interface. The stack port connects to the GigaStack GBIC multidrop backbone. If you try to enable CSUF on a Fast Ethernet or a copper-based Gigabit Ethernet port, you receive an error message.

If CSUF is already enabled on an interface and you try to enable it on another interface, you receive an error message. You must disable CSUF on the first interface before enabling it on a new interface.

Examples

This example shows how to enable CSUF on the GBIC interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree stack-port
```

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

Related Commands

Command	Description
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
spanning-tree uplinkfast	Accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.

spanning-tree transmit hold-count

Use the **spanning-tree transmit hold-count** 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*]

Syntax Description

Number of BPDUs sent every second. The range is 1 to 20.

Defaults

The default is 6.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEC	This command was introduced

Usage Guidelines

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.

Examples

This example shows how to set the transmit hold count to 8:

```
Switch(config)# spanning-tree transmit hold-count8
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Related Commands

Command	Description
show spanning-tree mst	Displays the multiple spanning-tree (MST) region configuration and status, including the transmit holdcount.

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**]

Syntax Description

max-update-rate *pkts-per-second*	(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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(13)EA1	The range for the pkts-per-second was changed from 0 to 65535 to 0 to 32000.

Usage Guidelines

Use this command only on access switches.

You can configure 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 the 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 switches over 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
show spanning-tree summary	Displays a summary of the spanning-tree port states.
spanning-tree stack-port	Enables cross-stack UplinkFast (CSUF) on an interface and accelerates the choice of a new root port when a link or switch fails or when spanning tree reconfigures itself.
spanning-tree vlan root primary	Forces this switch to be the root switch.

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

vlan-id	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.
forward-time *seconds*	Set the forward-delay time for the specified spanning-tree instance. The forwarding time determines how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time *seconds*	Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age *seconds*	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.
priority *priority*	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. 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.
root primary	Force this switch to be the root switch.
root secondary	Set this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	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.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	The **priority** *priority* range changed from 1 to 65535 to 1 to 61440 (in increments of 4096).
12.1(13)EA1	The value for the *vlan-id* variable was changed.

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 switch does not detect and prevent loops in a VLAN if STP is disabled for that VLAN.

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 the STP 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 primary** command, the switch recalculates the **forward-time, hello-time**, **max-age**, and **priority** settings. If you previously configured these parameters, the switch overrides and recalculates them.

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
```

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

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled ports or enables the Port Fast feature on all nontrunking ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface in all its associated VLANs.
spanning-tree uplinkfast	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 Mbps or 10/100/1000 Mbps 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

Note You cannot configure speed or duplex mode on Gigabit Interface Converter (GBIC) ports, but for certain types of GBICs, you can configure speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation.

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
1000	Port runs at 1000 Mbps. This option is valid and visible only on Gigabit Ethernet (Tx) ports.
auto	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the **10**, **100**, or **1000** keywords with the **auto** keyword, the port only autonegotiates at the specified speeds.
nonegotiate	Autonegotiation is disabled and the port runs at 1000 Mbps. This option is valid and visible only on 1000BASE-SX, -LX, and -ZX GBIC ports. Gigastack GBICs and 1000BASE-T GBICs do not support disabling of autonegotiation.

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(6)EA1	The **1000** and **nonegotiate** keywords were added.
12.1(22)EA1	Support for the **10**, **100**, and **1000** keywords with the auto keyword was added.

Usage Guidelines

You can configure Fast Ethernet port speed to either 10 or 100 Mbps. You can configure Gigabit Ethernet port speed to 10, 100, or 1000 Mbps. You cannot configure speed on Gigabit Interface Converter (GBIC) interfaces, but for 1000BASE-SX, -LX, or -ZX GBICs, you can configure speed to not negotiate (**nonegotiate**) if connected to a device that does not support autonegotiation.

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 the speed is set to **auto** and the **10**, **100**, or **1000** keywords are also used, the port only autonegotiates at the specified speeds.

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, configure duplex and speed on the other side; do use the **auto** setting on the supported side.

If both the speed and duplex are set to specific values, autonegotiation is disabled.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Note For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

Examples

This example shows how to set the specified interface to 100 Mbps:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mbps:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# speed auto 10 100
```

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

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

Related Commands

Command	Description
duplex	Specifies the duplex mode of operation for Fast Ethernet and Gigabit Ethernet ports.
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface

storm-control

Use the **storm-control** interface configuration command to configure broadcast, multicast, or unicast storm control with a specific suppression-level threshold 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*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

no storm-control {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

Syntax Description

broadcast	Enable broadcast storm control on the interface.
multicast	Enable multicast storm control on the interface.
unicast	Enable unicast storm control on the interface.
level *level* [*level-low*]	Specify the rising and falling suppression levels as a percentage of total bandwidth of the port. • *level*—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 *level* is reached. • *level-low*—(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.
level pps *pps* [*pps-low*]	Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port. • *pps*—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for *pps* is reached. • *pps-low*—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value. You can use metric suffixes such as k, m, and g for large number thresholds.
action {**shutdown** | **trap**}	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: • **shutdown**—Disables the port during a storm. • **trap**—Sends an SNMP trap when a storm occurs.

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

Release	Modification
12.1(8)EA1	This command was introduced. It replaces the **switchport broadcast**, **switchport multicast**, and **switchport unicast** interface configuration commands.
12.1(22)EA1	The **level** *level* [.*level*] option was replaced with the **level** *level* [*level-low*] option. The **pps** *pps pps-low* options were added.
12.2(25)SE	The *pps-low* option was made an optional parameter, and the range was changed. The **action** {**shutdown** | **trap**} keywords were added.

Usage Guidelines

Storm control is supported only on physical interfaces; it is not supported on EtherChannel port channels, even though it is available in the CLI.

The storm-control suppression level can be entered as a percentage of total bandwidth or as a rate in packets 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 If a multicast storm control suppression level is exceeded on a switch, all traffic (multicast, unicast, and broadcast) is blocked until the multicast traffic rate drops below the threshold. Only spanning-tree packets are passed. If the broadcast or the unicast storm control suppression level is exceeded, only that type of traffic is blocked until the rate drops below the threshold.

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.

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
show storm-control	Displays broadcast, multicast, or unicast storm-control settings on all interfaces or on a specified interface.

switchcore

Use the **switchcore** global configuration command to reserve switch resources for high-priority traffic or to give buffer storage more priority than packet retrieval. Use the **no** form of this command to return to the default setting.

switchcore {**resource-allocation priority** | **wirespeed-store**}

no switchcore {**resource-allocation priority** | **wirespeed-store**}

Syntax Description

resource-allocation priority	Reserve switch resources for high-priority traffic. Lower-priority traffic is likely to be rejected during times of congestion.
wirespeed-store	Reserve bandwidth for buffer storage to accommodate broadcast and multicast storms.

Defaults

When quality of service (QoS) is disabled, both the **resource-allocation priority** and the **wirespeed-store** options are disabled.

When QoS is enabled, resource-allocation priority is enabled, and wirespeed store is disabled.

Use the **resource-allocation priority** keywords when you want to reserve some switch buffers for high-priority traffic. Use the **wirespeed-store** keywords when you want to allocate more switch bandwidth to frame storage than to frame retrieval; this is only needed when you expect lots of broadcast and multicast traffic on the switch, and you want frame retrieval to be the dominant operation.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

You must globally enable QoS by using the **mls qos** global configuration command before the **switchcore** global configuration command takes effect.

Examples

This example shows how to disable resource-allocation priority:

```
Switch(config)# no switchcore resource-allocation priority
```

This example shows how to enable QoS and enable the wirespeed-store:

```
Switch(config)# mls qos
Switch(config)# switchcore wirespeed-store
```

You can verify your settings by entering the **show controllers switch** {**resource-allocation priority** | **wirespeed-store**} privileged EXEC command.

Related Commands

Command	Description
show controllers switch resource-allocation priority	Displays the setting of the resource-allocation priority feature or the wirespeed-store.
show controllers switch wirespeed-store	

switchport

Use the **switchport** interface configuration command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration. Use the **no** form of this command to put an interface in Layer 3 mode.

switchport

no switchport

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.

Note If an interface is to be configured as a Layer 3 interface, you must first enter the **switchport** command with no keywords to configure the interface as a Layer 2 port. Then you can enter additional switchport commands with keywords.

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all interfaces are in Layer 2 mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Entering the **no switchport** command shuts the port down and then re-enables it, which might generate messages on the device to which the port is connected.

Examples

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

```
Switch(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2-switched interface:

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

Note The **switchport** command without keywords is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.

switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access or dynamic-access port. If the mode is set to **access**, the port operates as a member of the configured 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

Syntax Description

vlan *vlan-id*	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.
vlan dynamic	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 obtain 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

Release	Modification
12.1(4)EA1	This command was introduced.

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 3550 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.
  - Tunnel ports.

Examples

This example shows how to cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN when in access mode:

```
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

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

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 {*interface-id*} **mmu primary vlan** *vlan-id*

switchport backup interface {*interface-id*} **preemption** [**forced** | **bandwidth** | **off**] | [**delay** *delay-time*]

no switchport backup interface {*interface-id*} **mmu primary vlan** *vlan-id*

no switchport backup interface {*interface-id*} **preemption** [**forced** | **bandwidth** | **off**] | [**delay**]

Syntax Description

interface-id	Specify 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.
mmu	Specifies configuring the mac move update (MMU) for a backup interface pair.
primary vlan *vlan-id*	The VLAN ID of the private-VLAN primary VLAN; valid range is 1 to 4094.
preemption	Specifies configuring a preemption scheme for a backup interface pair.
forced	(Optional) Specifies the interface always preempts the backup.
bandwidth	(Optional) Specifies the interface with the higher available bandwidth always preempts the backup.
off	(Optional) Specifies no preemption occurs from backup to active.
delay *delay-time*	(Optional) Specifies a preemption delay; valid values are 1 to 300 seconds.

Note Though visible in the command-line help, VLAN interfaces are not supported.

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	This command was introduced.

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 takes over traffic forwarding.
- 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 primary 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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2
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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 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 fastethernet1/0/1
Switch(conf-if)# switchport backup interface fastethernet1/0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

You can verify your setting by entering the **show interfaces switchport backup** privileged EXEC command.

Related Commands

Command	Description
show interfaces [*interface-id*] **switchport backup**	Displays the configured Flex Links and their status on the switch or for the specified interface.

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 return to the default setting.

switchport block {**multicast** | **unicast**}

no switchport block {**multicast** | **unicast**}

Syntax Description

multicast	Specify that unknown multicast traffic should be blocked.
unicast	Specify that unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic are not blocked.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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 non-protected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

Note For more information about blocking packets, see the software configuration guide for this release.

Examples

This example shows how to block unknown multicast traffic on an interface:

```
Switch(config-if)# switchport block multicast
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.

switchport broadcast

This is an obsolete command.

In past releases, the **switchport broadcast** interface configuration command was used to set the broadcast suppression level on the interface. This command is replaced by the **storm-control broadcast** interface configuration command.

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	This command was replaced by the **storm-control** command.

Related Commands

Command	Description
show storm-control broadcast	Displays broadcast suppression settings on an interface or on all interfaces.
storm-control	Sets broadcast, multicast, or unicast storm control on an interface with the specified threshold level.
switchport multicast	Obsolete command. Replaced by the **storm-control multicast** interface configuration command.
switchport unicast	Obsolete command. Replaced by the **storm-control unicast** interface configuration command.

switchport host

Use the **switchport host** interface configuration command on the switch to optimize a Layer 2 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

Release	Modification
12.1(20)EA1	This command was introduced.

Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets the 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 to start packet forwarding.

The **no switchport host** command has no affect. To return an interface to a configuration not optimized as a host connection, you can manually reconfigure switchport mode, spanning-tree Port Fast, and channel grouping. You can also use the **default interface** *interface-id* global config command to return the interface to its default state. However, this command also returns other interface configuration to the default.

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 the effects of the command by entering the **show interfaces** *interface-id* **switchport** or **show running-config interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including switchport mode.
show running-config interface *interface-id*	Displays the running configuration on the interface.

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** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}

no switchport mode {**access**| **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}

Syntax Description

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** 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.
dot1q-tunnel	Set the port as an IEEE 802.1Q tunnel port.
dynamic auto	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link.
dynamic desirable	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk	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 desirable**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **dot1q-tunnel** keyword was added.

Usage Guidelines

A configuration that uses the **access**, **trunk,** or **dot1q-tunnel** 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.

To autonegotiate trunking, the interfaces must be in the same 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.
- With GigaStack GBICs, dynamic trunking is only supported when two switches are connected by a single GigaStack GBIC link. If trunking is required when more than two switches in a stack are connected by GigaStack GBIC links, you must manually configure trunking in this manner:
  - Manually shut down the GigaStack port by using the **shutdown** interface configuration command.
  - Manually configure trunk mode on the GigaStack port by using the **switchport mode trunk** interface configuration command on both GBIC interfaces to cause the interfaces to become trunks.
  - Use the **no shutdown** interface configuration command to bring up the GigaStack port.

When you enter **dot1q-tunnel**, the port is set unconditionally as an IEEE 802.1Q tunnel port.

Access port, trunk ports, and tunnel ports are mutually exclusive.

Any IEEE 802.1Q encapsulated IP packets received on a tunnel port can be filtered by MAC ACLs, but not by IP ACLs. This is because the switch does not recognize the protocol inside the IEEE 802.1Q header. This restriction applies to router ACLs, port ACLs and VLAN maps.

The IEEE 802.1x authentication feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x authentication on a trunk 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 trunk, the port mode is not changed.
- 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, the port mode is not changed.
- 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.

Configuring a port as an IEEE 802IEEE 802.1Q tunnel port has these limitations:

- IP routing and fallback bridging are not supported on tunnel ports.
- Tunnel ports do not support IP access control lists (ACLs).
- If an IP ACL is applied to a trunk port in a VLAN that includes tunnel ports, or if a VLAN map is applied to a VLAN that includes tunnel ports, packets received from the tunnel port are treated as non-IP packets and filtered with MAC access lists.
- Layer 3 QoS ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports.

Note For more information about configuring IEEE 802.1Q tunnel ports, see the software configuration guide for this release.

Examples

This example shows how to configure a port for access mode:

```
Switch(config-if)# switchport mode access
```

This example shows how set the interface to dynamic desirable mode:

```
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config-if)# switchport mode trunk
```

This example shows how to configure a port for as an IEEE 802.1Q tunnel port:

```
Switch(config-if)# switchport mode dot1q-tunnel
```

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

Command	Description
show dot1q-tunnel	Displays information about IEEE 802.1Q tunnel ports on the switch.
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport access	Configures a port as a static-access or dynamic-access port.
switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.

switchport multicast

This is an obsolete command.

In past releases, the **switchport multicast** interface configuration command was used to set the multicast suppression level on the interface. This command is replaced by the **storm-control multicast** interface configuration command.

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	This command was replaced by the **storm-control** command.

Related Commands

Command	Description
show storm-control multicast	Displays multicast suppression settings on an interface or on all interfaces.
storm-control	Sets broadcast, multicast, or unicast storm control on an interface with the specified threshold level.
switchport broadcast	Obsolete command. Replaced by the **storm-control broadcast** interface configuration command.
switchport unicast	Obsolete command. Replaced by the **storm-control unicast** interface configuration command.

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 determine trunking status.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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.

Examples

This example shows how to cause a port interface to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the **mode** set):

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

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	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**}]

no switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

Syntax Description

aging	(Optional) See the **switchport port-security aging** command.
mac-address *mac-address*	(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.
vlan *vlan-id*	(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.
vlan access	(Optional) On an access port, specify the VLAN as an access VLAN.
vlan voice	(Optional) On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
mac-address sticky [*mac-address*]	(Optional) Enable the interface for *sticky learning* by entering only the **mac-address sticky** 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 *mac-address* to specify a sticky secure MAC address.
maximum *value*	(Optional) The maximum number of available addresses is determined by the active Switch Database Management (SDM) template. The default is 1.
vlan [*vlan-list*]	(Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the **vlan** keyword is not entered, the default value is used. • **vlan**—set a per-VLAN maximum value. • **vlan** *vlan-list*—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.

violation	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is **shutdown**.
protect	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. **Note** 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.
restrict	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.
shutdown	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 **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Port security is disabled.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

Sticky learning is disabled.

The default violation mode is **shutdown**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8)EA1	This command was introduced.
12.1(11)EA1	The **mac-address sticky** [*mac-address*] option was added.
12.1(14)EA1	The **vlan** *vlan-id* and **vlan** *vlan-list* keywords were added.
12.2(25)SEB	The **access** and **voice** keywords were added.

Usage Guidelines

A secure port has these 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 routed 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.
- 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 Cisco IP phone requires up to two MAC addresses. 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 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.

If you enable port security on a voice VLAN port and connect a single PC to the Cisco IP phone, you should set the maximum allowed secure addresses on the port to two. If you enable port security on a voice VLAN port and 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 IP phone.

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, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

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.

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, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration. If you remove the sticky MAC addresses from the running configuration, the sticky secure MAC addresses are removed from the running configuration and the address table.
- 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 fastethernet0/1
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 on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
```

This example shows how to enable sticky learning:

```
Switch(config-if)# switchport port-security mac-address sticky
```

This example shows how to configure a secure MAC address on a trunk port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 9
```

This example shows how to configure a maximum of 5 secure MAC addresses on VLAN 9:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport port-security maximum 5 vlan 9
```

You can verify the settings for all secure ports or the specified port by using the **show port-security** privileged EXEC command.

Related Commands

Command	Description
clear port-security	Deletes from the MAC address table a specific secure address or all the secure addresses on an interface.

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 statically configured secure addresses on a particular port. Use the **no** form of this command to return to the default settings.

switchport port-security aging {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

no switchport port-security aging {**static** | **time** | **type**}

Syntax Description

static	Enable aging for statically configured secure addresses on this port.
time *time*	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.
type absolute	Set the aging type as absolute aging. All the secure addresses on this port age out after the time (minutes) specified and are removed from the secure address list.
type inactivity	Set the aging type as inactivity aging. 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

Release	Modification
12.1(9)EA1	This command was introduced.

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 specific secure MAC addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted. When the device sends traffic again, the deleted secure addresses are relearned.

Note The absolute aging time could vary by 1 minute, depending on the sequence of the system timer.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become 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 a port:

```
Switch(config)# interface fastethernet0/1
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 a port:

```
Switch(config)# interface fastethernet0/2
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-if)# no switchport port-security aging static
```

Related Commands

Command	Description
show port-security	Displays the port security settings defined for the port.
switchport port-security	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

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

Syntax Description

cos *value*	Set the IP phone port to override the priority received from the PC or the attached device. The class of service (CoS) value is a number from 0 to 7. Seven is the highest priority. The default is 0.
trust	Set the IP phone port to trust the priority received from the PC or the attached device.

Defaults

The port priority is not set, and the default value for untagged frames received on the port is 0.

The IP phone connected to the port is set to not trust the priority of incoming traffic and overrides the priority with the CoS value of 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(13)EA1	The **none** keyword was removed and was replaced by the **trust** keyword.

Usage Guidelines

In Cisco IOS Release 12.1(13)EA1 or later, the **trust** keyword replaces the **none** keyword. To instruct the IP Phone to not trust the priority, you can use the **no switchport priority extend** or the **switchport priority extend cos 0** interface configuration command. In software releases earlier than Cisco IOS Release 12.1(13)EA1, use the **switchport priority extend none** 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-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
show interfaces	Displays the administrative and operational status of a switching (nonrouting) port.
switchport voice vlan	Configures the voice VLAN on the port.

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 return to the default setting.

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

Release	Modification
12.1(4)EA1	This command was introduced.

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 unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

Protected ports are supported on IEEE 802.1Q trunks.

Examples

This example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
```

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

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport block	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*} | {**encapsulation** {**dot1q** | **isl** | **negotiate**}} | {**native vlan** *vlan-id*} | {**pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** *vlan-list*} | {**encapsulation** {**dot1q** | **isl** | **negotiate**}} | {**native vlan** *vlan-id*} | {**pruning vlan** *vlan-list*}

Syntax Description

allowed vlan *vlan-list*	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 *vlan-list* format. The **none** keyword is not valid. The default is **all**.
encapsulation dot1q	Set the encapsulation format on the trunk port to IEEE 802.1Q. With this format, the switch supports simultaneous tagged and untagged traffic on a port.
encapsulation isl	Set the encapsulation format on the trunk port to Inter-Switch Link (ISL). The switch encapsulates all received and sent packets with an ISL header and filters native frames received from an ISL trunk port.
encapsulation negotiate	Specify that if Dynamic Inter-Switch Link (DISL) and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan *vlan-id*	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.
pruning vlan *vlan-list*	Set the list of VLANs that are eligible for VTP pruning when in trunking mode. The **all** 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. The range is 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. The range is 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.) The range is 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

The default encapsulation is negotiate.

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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(14)EA1	The **allowed vlan** *vlan-list* **add**, **remove** and **except** keywords were modified to accept the VLAN 1 and VLANs 1002 to 1005 values.

Usage Guidelines

Encapsulation:

- The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and IEEE 802.1Q formats.
- You cannot configure one end of the trunk as an IEEE 802.1Q trunk and the other end as an ISL or nontrunk port. However, you can configure one port as an ISL trunk and a different port on the same switch as an IEEE 802.1Q trunk.

- If you enter the **negotiate** keywords and DTP negotiation does not resolve the encapsulation format, ISL is the selected format. The **no** form of the command resets the trunk encapsulation format to the default.
- The **no** form of the **encapsulation** command resets the encapsulation format to the default.

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. This is known as VLAN 1 minimization. VLAN 1 minimization disables VLAN 1 (the default VLAN on all Cisco switch trunk ports) on an individual VLAN trunk link. As a result, no user traffic, including spanning-tree advertisements, is sent or received on VLAN 1.

  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 cause a port interface configured as a switched interface to encapsulate in IEEE 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Switch(config-if)# switchport trunk encapsulation dot1q
```

This example shows how to configure VLAN 3 as the default port to send all untagged traffic:

```
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-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-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.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport unicast

This is an obsolete command.

In past releases, the **switchport unicast** interface configuration command was used to set the multicast suppression level on the interface. This command is replaced by the **storm-control unicast** interface configuration command.

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(8)EA1	This command was replaced by the **storm-control** command.

Related Commands

Command	Description
show storm-control unicast	Displays unicast suppression settings on an interface or on all interfaces.
storm-control	Sets broadcast, multicast, or unicast storm control on an interface with the specified threshold level.
switchport broadcast	Obsolete command. Replaced by the **storm-control broadcast** interface configuration command.
switchport multicast	Obsolete command. Replaced by the **storm-control multicast** interface configuration command.

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

Syntax Description

vlan-id	VLAN used for voice traffic. The range is 1 to 4094.
dot1p	The telephone uses priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
none	The telephone is not instructed through the CLI about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged	The telephone does not tag frames and uses VLAN 4095. The default for the telephone is untagged.

Defaults

The switch default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

You should configure voice VLAN on access ports.

Before you enable voice VLAN, we recommend 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 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 on 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:

```
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

Command	Description
show interfaces *interface-id* **switchport**	Displays the administrative and operational status of a switching (nonrouting) port.
switchport priority extend	Determines 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 the switch. Use the **no** form of this command to return to the default setting.

system mtu *bytes*

no system mtu

Syntax Description

bytes	Packet size in bytes. The range is 1500 to 2000 bytes for Gigabit Ethernet switches and 1500 to 1546 bytes for Fast Ethernet switches.

Defaults

The default MTU size is 1500 bytes.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

When you use this command to change the MTU size, you must reset the switch before the new configuration takes effect.

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 1500 bytes, no matter what value was entered with the **system mtu** command. Although frames that are forwarded or routed typically are not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, Telnet, or routing protocols.

Examples

This example shows how to set the maximum packet size for a Gigabit Ethernet switch to 1580 bytes:

```
Switch(config)# system mtu 1580
Switch(config)# exit
Switch# reload
```

This example shows the response when you try to set a Fast Ethernet switch to an out-of-range number:

```
Switch(config)# system mtu 1580
                           ^
% Invalid input detected at '^' marker.
```

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

Related Commands

Command	Description
show system mtu	Displays the maximum packet size set for the switch.

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

interface *interface-id*	(Optional) Specify an interface on the source or destination switch.
source-mac-address	Specify the MAC address of the source switch in hexadecimal format.
destination-mac-address	Specify the MAC address of the destination switch in hexadecimal format.
vlan *vlan-id*	(Optional) Specify the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. The range is 1 to 4094.
detail	(Optional) Specify that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to functional 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[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5                 (2.2.5.5        )  :    Fa0/3 => 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[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[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2950G-24-EI / 2.2.6.6 :
        Fa0/1 [auto, auto] => Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 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[WS-C2950G-24-EI] (2.2.6.6)
con6 (2.2.6.6) :Fa0/1 => Fa0/3
con5                 (2.2.5.5        )  :    Fa0/3 => 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[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[WS-C2950G-24-EI] (2.2.5.5)
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/1 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 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
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

Command	Description
traceroute mac ip	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** 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

source-ip-address	Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
destination-ip-address	Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
source-hostname	Specify the IP hostname of the source switch.
destination-hostname	Specify the IP hostname of the destination switch.
detail	(Optional) Specify that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to functional properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects an 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.

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 / WS-C2950G-24-EI / 2.2.6.6 :
        Fa0/1 [auto, auto] => Fa0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 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) :Fa0/1 => Fa0/3
con5                 (2.2.5.5        )   :    Fa0/3 => 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

Command	Description
traceroute mac	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 by the **class** or the **class-map** 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

cos	(Optional) Classify ingress packets by using the packet class of service (CoS) values. For untagged packets, the port default CoS value is used.
dscp	(Optional) Classify ingress packets by using the packet Differentiated Services Code Point (DSCP) values (most significant 6 bits of 8-bit service-type field). For non-IP packets, 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.
ip-precedence	(Optional) Classify ingress packets by using the packet IP-precedence values (most significant 3 bits of 8-bit service-type field). For non-IP packets, 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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from others. 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 on specific interfaces 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.

You cannot use the **service-policy** interface configuration command to attach policy maps that contain these elements to an egress interface:

- **set** or **trust** policy-map class configuration commands. Instead, you can use the **police** policy-map class configuration command to mark down (reduce) the DSCP value at the egress interface.
- Access control list (ACL) classification.
- Per-port per-VLAN classification.

The only match criterion in a policy map that can be attached to an egress interface is the **match ip dscp** *dscp-list* class-map configuration command.

If you specify **trust cos**, QoS derives the internal DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.

If you specify **trust dscp**, QoS derives the internal DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the internal DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the internal DSCP value by using the default port CoS value. In either case, the internal DSCP value is derived from the CoS-to-DSCP map.

If you specify **trust ip-precedence**, QoS derives the internal DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the internal DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the internal DSCP value by using the default port CoS value. In either case, the internal DSCP value is derived from the CoS-to-DSCP map.

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

Command	Description
class	Defines a traffic classification for the policy to act on.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy.
show policy-map	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 this 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

aggressive	Enable UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enable UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	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 1 to 90 seconds.

Defaults

UDLD is disabled on all fiber-optic interfaces.

The message timer is set at 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(25)SEC	The range for *message-timer-interval* was changed from 7 to 90 seconds to 1 to 90 seconds.

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 **udld port disable** 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

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	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**]

Syntax Description

aggressive	(Optional) Enable UDLD in aggressive mode on the specified interface.

Defaults

On fiber-optic interfaces, UDLD is neither 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.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(14)EA1	The **port** keyword was added. The **enable** keyword was removed.
12.1(20)EA2	The **disable** keyword was removed.

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.

If the switch software detects a Gigabit Interface Converter (GBIC) module change and the port changes from fiber optic to nonfiber optic or vice versa, all configurations are maintained.

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 an interface:

```
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

Command	Description
show running-config	Displays the running configuration on the switch. For syntax information, for more information about configuring an SDM template **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	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 shutdown 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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and might shutdown 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
show running-config	Displays the running configuration on the switch. For syntax information, for more information about configuring an SDM template **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.

vlan (global configuration)

Use the **vlan** global configuration command to add a VLAN and enter the config-vlan mode. Use the **no** form of this command to delete the VLAN.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. The range is 1 to 4094; do not enter leading zeros. 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

Release	Modification
12.1(9)EA1	This command was introduced.
12.1(11)EA1	The **remote-span** configuration command was added.

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 by entering the **copy running-config startup-config** privileged EXEC command.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the switch, the configuration is determined 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 the image on the switch or the configuration file is earlier than Cisco IOS Release 12.1(9)EA1, the switch reboots with information in the VLAN database.

Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database.

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 config-vlan command supported on extended-range VLANs is **mtu** *mtu-size*. 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:
  - **srb** (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 2-31 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.

Note Though visible in the command-line interface, the **private-vlan** command is not supported.

- **remote-span**: adds the Remote SPAN (RSPAN) feature to the 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. The new RSPAN VLAN is propagated by VTP for VLAN-IDs that are lower than 1024. Learning is disabled on the VLAN. Only Layer 2 switch protocols will be processed by the CPU. Broadcast packets, multicast packets and unicast packets addressed directly to the switch will be flooded on the VLAN but will not be forwarded to the CPU.
- **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 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 2-31 Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**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*
FDDI	**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*
FDDI-NET	**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* If VTP v2 mode is disabled, do not set the **stp type** to **auto**.
Token Ring	VTP v1 mode is enabled. **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*
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tokenring, state** {**suspend** | **active**}, **said** *said-value*, **mtu** *mtu-size*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb** | **srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable** | **disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring-NET	VTP v1 mode is enabled. **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*
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. **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*

Table 2-32 describes the rules for configuring VLANs.

Table 2-32 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.

Table 2-32 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
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
show running-config vlan	Displays all or a range of VLAN-related configurations on the switch.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
vlan (VLAN configuration)	Configures normal-range VLANs in the VLAN database.

vlan (VLAN configuration)

Use the **vlan** VLAN configuration command to configure VLAN characteristics for a normal-range VLAN (VLAN IDs 1 to 1005) in the VLAN database. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command without additional parameters to delete a VLAN. Use the **no** form with parameters to change its configured characteristics.

vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

no vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

Extended-range VLANs (with VLAN IDs from 1006 to 4094) cannot be added or modified by using these commands. To add extended-range VLANs, use the **vlan (global configuration)** command to enter config-vlan mode.

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.

Syntax Description

vlan-id	ID of the configured VLAN. The range is 1 to 1005 and must be unique within the administrative domain. Do not enter leading zeros.
are *are-number*	(Optional) Specify 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. If no value is entered, 0 is assumed to be the maximum.
backupcrf {**enable** | **disable**}	(Optional) Specify 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.
bridge *bridge-number*| **type** {**srb** | **srt**}	(Optional) Specify 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 **type** keyword applies only to TrCRF VLANs and is one of these: • **srb** (source-route bridging) • **srt** (source-route transparent) bridging VLAN

media {**ethernet** | **fddi** | **fd-net** | **tokenring** | **tr-net**}	(Optional) Specify the VLAN media type. Table 2-33 lists the valid syntax for each media type. • **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 v2 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*	(Optional) Specify the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190.
name *vlan-name*	(Optional) Specify the VLAN name, an ASCII string from 1 to 32 characters that must be unique within the administrative domain.
parent *parent-vlan-id*	(Optional) Specify 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.
ring *ring-number*	(Optional) Specify the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
said *said-value*	(Optional) Enter the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294 and must be unique within the administrative domain.
state {**suspend** | **active**}	(Optional) Specify the VLAN state: • If **active**, the VLAN is operational. • If **suspend**, the VLAN is suspended. Suspended VLANs do not pass packets.
ste *ste-number*	(Optional) Specify the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13.
stp type {**ieee** | **ibm** | **auto**}	(Optional) Specify the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLAN. • **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*	(Optional) Specify 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. Zero is assumed if no value is specified.

Table 2-33 shows the valid syntax options for different media types.

Table 2-33 Valid Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**vlan** *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI	**vlan** *vlan-id* [**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*]
FDDI-NET	**vlan** *vlan-id* [**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*] If VTP v2 mode is disabled, do not set the **stp type** to **auto**.
Token Ring	VTP v1 mode is enabled. **vlan** *vlan-id* [**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*]
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**bridge type** {**srb** | **srt**}] [**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
Token Ring-NET	VTP v1 mode is enabled. **vlan** *vlan-id* [**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*]
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. **vlan** *vlan-id* [**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*]

Table 2-34 describes the rules for configuring VLANs.

Table 2-34 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.

Table 2-34 VLAN Configuration Rules (continued)

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
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).

Defaults

The ARE value is 7.

Backup CRF is disabled.

The bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs.

The **media** type is **ethernet**.

The default *mtu size* is 1500 bytes.

The *vlan-name* variable is *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.

The parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For TrCRF VLANs, you must specify a parent VLAN ID. 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.

The *ring number* for Token Ring VLANs is 0. For FDDI VLANs, there is no default.

The *said value* is 100000 plus the VLAN ID.

The state is **active**.

The STE value is 7.

The STP type is **ieee** for FDDI-NET and **ibm** for Token Ring-NET VLANs. For FDDI and Token Ring VLANs, the default is no type specified.

The *tb-vlan1-id* and *tb-vlan2-id* variables are zero (no translational bridging).

Command Modes

VLAN configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(13)EA1	The value for *vlan-id* variable was changed.

Usage Guidelines

You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 1005.

Note To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan** global configuration command.

VLAN configuration is always saved in the VLAN database. If VTP mode is transparent, it is also saved in the switch running configuration file, along with the VTP mode and domain name. You can then save it in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

When you save VLAN and VTP configuration in the startup configuration file and reboot the switch, the configuration is determined 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 VLAN database information.
- If the image on the switch or the configuration file is earlier than Cisco IOS Release 12.1(9)EA1, the switch reboots with information in the VLAN database.

The following are the results of using the **no vlan** commands:

- When the **no vlan** *vlan-id* form is used, the VLAN is deleted. Deleting VLANs automatically resets to zero any other parent VLANs and translational bridging parameters that refer to the deleted VLAN.
- When the **no vlan** *vlan-id* **bridge** form is used, the VLAN source-routing bridge number returns to the default (0). The **vlan** *vlan-id* **bridge** command is used only for FDDI-NET and Token Ring-NET VLANs and is ignored in other VLAN types.
- When the **no vlan** *vlan-id* **media** form is used, the media type returns to the default (**ethernet**). Changing the VLAN media type (including the **no** form) resets the VLAN MTU to the default MTU for the type (unless the **mtu** keyword is also present in the command). It also resets the VLAN parent and translational bridging VLAN to the default (unless the **parent**, **tb-vlan1**, or **tb-vlan2** are also present in the command).
- When the **no vlan** *vlan-id* **mtu** form is used, the VLAN MTU returns to the default for the applicable VLAN media type. You can also modify the MTU by using the **media** keyword.
- When the **no vlan** *vlan-id* **name** *vlan-name* form is used, the VLAN name returns to the default name (*VLANxxxx*, where *xxxx* represent four numeric digits [including leading zeros] equal to the VLAN ID number).

- When the **no vlan** *vlan-id* **parent** form is used, the parent VLAN returns to the default (0). The parent VLAN resets to the default if the parent VLAN is deleted or if the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.
- When the **no vlan** *vlan-id* **ring** form is used, the VLAN logical ring number returns to the default (0).
- When the **no vlan** *vlan-id* **said** form is used, the VLAN SAID returns to the default (100,000 plus the VLAN ID).
- When the **no vlan** *vlan-id* **state** form is used, the VLAN state returns to the default (**active)**.
- When the **no vlan** *vlan-id* **stp type** form is used, the VLAN spanning-tree type returns to the default (**ieee**).
- When the **no vlan** *vlan-id* **tb-vlan1** or **no vlan** *vlan-id* **tb-vlan2** form is used, the VLAN translational bridge VLAN (or VLANs, if applicable) returns to the default (0). Translational bridge VLANs must be a different VLAN type than the affected VLAN, and if two are specified, the two must be different VLAN types from each other. A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted, if the **media** keyword changes the VLAN type, or if the **media** keyword changes the VLAN type of the corresponding translation bridge VLAN.

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** or **apply** vlan configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

```
Switch(vlan)# vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting....
```

This example shows how to modify an existing VLAN by changing its name and MTU size:

```
Switch(vlan)# no vlan name engineering mtu 1200
```

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

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.
vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

vlan access-map

Use the **vlan access-map** global configuration command to create or modify a VLAN map entry for VLAN packet filtering. This entry changes the mode to the VLAN access map configuration. Use the **no** form of this command to delete a VLAN map entry. Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

Syntax Description

name	Name of the VLAN map.
number	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Defaults

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access map configuration mode, these commands are available:

- **action**: sets the action to be taken (forward or drop).
- **default**: sets a command to its defaults
- **exit**: exits from VLAN access-map configuration mode
- **match**: sets the values to match (IP address or MAC address).
- **no**: negates a command or set its defaults

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

In global configuration mode, use the **vlan filter** interface configuration command to apply the map to one or more VLANs.

Note For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example shows how to create a VLAN map named *vac1* and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

This example shows how to delete VLAN map *vac1*:

```
Switch(config)# no vlan access-map vac1
```

Related Commands

Command	Description
action	Sets the action for the VLAN access map entry.
match (access-map configuration))	Sets the VLAN map to match packets against one or more access lists.
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan filter	Applies the VLAN access map to one or more VLANs.

vlan database

Use the **vlan database** privileged EXEC command to enter VLAN configuration mode. From this mode, you can add, delete, and modify VLAN configurations for normal-range VLANs and globally propagate these changes by using the VLAN Trunking Protocol (VTP). Configuration information is saved in the VLAN database.

vlan database

Note VLAN configuration mode is only valid for VLAN IDs 1 to 1005.

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You can use the VLAN database configuration commands to configure VLANs 1 to 1005. To configure extended-range VLANs (VLAN IDs 1006 to 4094), use the **vlan (global configuration)** command to enter config-vlan mode. You can also configure VLAN IDs 1 to 1005 by using the **vlan** global configuration command.

To return to the privileged EXEC mode from the VLAN configuration mode, enter the **exit** command.

Note This command mode is different from other modes because it is session-oriented. When you add, delete, or modify VLAN parameters, the changes are not applied until you exit the session by entering the **apply** or **exit** command. When the changes are applied, the VTP configuration version is incremented. You can also *not* apply the changes to the VTP database by entering **abort**.

When you are in VLAN configuration mode, you can access the VLAN database and make changes by using these commands:

- **vlan**: accesses subcommands to add, delete, or modify values associated with a single VLAN. For more information, see the **vlan (VLAN configuration)** command.
- **vtp**: accesses subcommands to perform VTP administrative functions. For more information, see the **vtp (VLAN configuration)** command.

When you have modified VLAN or VTP parameters, you can use these editing buffer manipulation commands:

- **abort**: exits the mode without applying the changes. The VLAN configuration that was running before you entered VLAN configuration mode continues to be used.
- **apply**: applies current changes to the VLAN database, increments the database configuration revision number, propagates it throughout the administrative domain, and remains in VLAN configuration mode.

  Note You cannot use this command when the switch is in VTP client mode.

- **exit**: applies all configuration changes to the VLAN database, increments the database configuration number, propagates it throughout the administrative domain, and returns to privileged EXEC mode.
- **no**: negates a command or set its defaults; valid values are **vlan** and **vtp**.
- **reset**: abandons proposed changes to the VLAN database, resets the proposed database to the implemented VLAN database on the switch, and remains in VLAN configuration mode.
- **show**: displays VLAN database information.
- **show changes** [*vlan-id*]: displays the differences between the VLAN database on the switch and the proposed VLAN database for all normal-range VLAN IDs (1 to 1005) or the specified VLAN ID (1 to 1005).
- **show current** [*vlan-id*]: displays the VLAN database on the switch or on a selected VLAN (1 to 1005).
- **show proposed** [*vlan-id*]: displays the proposed VLAN database or a selected VLAN (1 to 1005) from the proposed database. The proposed VLAN database is not the running configuration until you use the **exit** or **apply** VLAN configuration command.

You can verify that VLAN database changes have been made or aborted by using the **show vlan** privileged EXEC command. This output is different from the **show** VLAN database configuration command output.

Examples

This example shows how to enter the VLAN configuration mode from the privileged EXEC mode and to display VLAN database information:

```
Switch# vlan database
Switch(vlan)# show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500
```

```
VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

<output truncated>
```

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

```
Switch(vlan)# show changes

DELETED:
  VLAN ISL Id: 4
    Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

DELETED:
  VLAN ISL Id: 6
    Name: VLAN0006
    Media Type: Ethernet
    VLAN 802.10 Id: 100006
    State: Operational
    MTU: 1500

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

This example shows how to display the differences between VLAN 7 in the current database and the proposed database:

```
Switch(vlan)# show changes 7

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

This is an example of output from the **show current 20** command. It displays only VLAN 20 of the current database.

```
Switch(vlan)# show current 20
VLAN ISL Id: 20
    Name: VLAN0020
    Media Type: Ethernet
    VLAN 802.10 Id: 100020
    State: Operational
    MTU: 1500
```

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs in the administrative domain.
shutdown vlan	Shuts down (suspends) local traffic on the specified VLAN.
vlan (global configuration)	Enters config-vlan mode for configuring normal-range and extended-range VLANs.

vlan dot1q tag native

Use the **vlan dot1q tag native** global configuration command to enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports. Use the **no** form of this command to return to the default setting.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Defaults

The IEEE 802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

When enabled, native VLAN packets going out all IEEE 802 IEEE 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out all IEEE 802.1Q trunk ports are not tagged.

You can use this command with the IEEE 802.1Q tunneling feature. This feature operates on an edge switch of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. You must use IEEE 802.1Q trunk ports for sending packets to the service-provider network. However, packets going through the core of the service-provider network might also be carried on IEEE 802.1Q trunks. If the native VLANs of an IEEE 802.1Q trunks match the native VLAN of a tunneling port on the same switch, traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that native VLAN packets on all IEEE 802.1Q trunk ports are tagged.

Note For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

Related Commands

Command	Description
show vlan dot1q tag native	Displays IEEE 802.1Q native VLAN tagging status.

vlan filter

Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs. Use the **no** form of this command to remove the map.

vlan filter *mapname* **vlan-list** *list*

no vlan filter *mapname* **vlan-list** *list*

Syntax Description

mapname	Name of the VLAN map entry.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The VLAN ID range is 1 to 4094.

Defaults

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN. If you apply a nonexistent VLAN map to a VLAN, a warning message appears.

Note For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *mac1* from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

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

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.

vmps reconfirm (privileged EXEC)

Use the **vmps 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).

vmps reconfirm

Syntax Description

This command has no arguments or keywords.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Examples

This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

Related Commands

Command	Description
show vmps	Displays VQP and VMPS information.
vmps reconfirm (global configuration)	Changes the reconfirmation interval for the VLAN Query Protocol (VQP) client.

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

Syntax Description

interval	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

Release	Modification
12.1(4)EA1	This command was introduced.

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
show vmps	Displays VQP and VMPS information.
vmps reconfirm (privileged EXEC)	Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS.

vmps retry

Use the **vmps 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.

vmps retry *count*

no vmps retry

Syntax Description

count	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.

Defaults

The default retry count is 3.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Examples

This example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Server Retry Count row.

Related Commands

Command	Description
show vmps	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*]

Syntax Description

ipaddress	IP address or host name of the primary or secondary VMPS servers. If you specify a host name, the Domain Name System (DNS) server must be configured.
primary	(Optional) Determines whether primary or secondary VMPS servers are being configured.

Defaults

No primary or secondary VMPS servers are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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
show vmps	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* | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}

no vtp {**file** | **interface | mode** | **password** | **pruning** | **version**}

Syntax Description

domain *domain-name*	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.
file *filename*	Specify the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface *name*	Specify the name of the interface providing the VTP ID updated for this device.
mode	Specify the VTP device mode as client, server, or transparent.
client	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.
server	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.
transparent	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 **copy running-config startup config** privileged EXEC command.
password *password*	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.
pruning	Enable VTP pruning on the switch.
version *number*	Set VTP version to version 1 or version 2.

Defaults

The default filename is *flash:vlan.dat*.

The default mode is server mode.

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

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **domain** and **mode** keywords were added. The **if-id** keyword was replaced by the **interface** keyword.
12.1(11)EA1	The **password**, **pruning**, and **version** keywords were added.

Usage Guidelines

When you save VTP mode and domain name and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are determined 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 determined by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.
- If the image on the switch or the configuration file is earlier than Cisco IOS Release 12.1(9)EA1, the switch reboots using the information in the VLAN database.

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.
- 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.
- 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.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

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.

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.

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 fastethernet
```

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
```

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

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (VLAN configuration)	Configures VTP domain-name, password, pruning, version, and mode.

vtp (privileged EXEC)

Use the **vtp** privileged EXEC command to configure the VLAN Trunking Protocol (VTP) password, pruning, and version. Use the **no** form of this command to return to the default settings.

vtp {**password** *password* | **pruning** | **version** *number*}

no vtp {**password** | **pruning** | **version**}

Note Beginning with release 12.1(11)EA1, these keywords are available in the **vtp** global configuration command. This command will become obsolete in a future release.

Syntax Description

password *password*	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.
pruning	Enable VTP pruning on the switch.
version *number*	Set VTP version to version 1 or version 2.

Defaults

No password is configured.

Pruning is disabled.

The default version is version 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

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.

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.

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.

You cannot save password, pruning, and version configuration in the switch configuration file.

Examples

This example shows how to configure the VTP domain password:

```
Switch# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch# vtp pruning
Pruning switched ON
```

This example shows how to enable version 2 mode in the VLAN database:

```
Switch# vtp version 2
```

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

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
vtp (global configuration)	Configures the VTP filename, interface, domain-name, and mode, which can be saved in the switch configuration file.
vtp (VLAN configuration)	Configures all VTP characteristics but cannot be saved to the switch configuration file.

vtp (VLAN configuration)

Use the **vtp** VLAN configuration command to configure VLAN Trunking Protocol (VTP) characteristics. You access VLAN configuration mode by entering the **vlan database** privileged EXEC command. Use the **no** form of this command to return to the default settings, disable the characteristic, or remove the password.

vtp {**domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | {**server** | **client** | **transparent**}}

no vtp {**client** | **password** | **pruning** | **transparent** | **v2-mode**}

Note VTP configuration in VLAN configuration mode is saved in the VLAN database when applied.

Syntax Description

domain *domain-name*	Set the VTP domain name by entering an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
password *password*	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.
pruning	Enable pruning in the VTP administrative domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.
v2-mode	Enable VLAN Trunking Protocol (VTP) version 2 in the administrative domains.
client	Place the switch in VTP client mode. 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.
server	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 it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	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.

Defaults

The default mode is server mode.

No domain name is defined.

No password is configured.

Pruning is disabled.

VTP version 2 (v2 mode) is disabled.

Command Modes

VLAN configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

If VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save the configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Follow these guidelines when setting VTP mode:

- The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.
- The **vtp server** command is the same as **no vtp client** or **no vtp transparent** 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, make 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 make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp transparent** command disables VTP from the domain but does not remove the domain from the switch.
- The VTP mode must be transparent for you to add extended-range VLANs or for the VTP and the VLAN configurations to be saved in the running configuration file.
- 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.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

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 receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name with the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter 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 reassign it only to a different domain.

Follow these guidelines when configuring a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When the **no vtp password** form of the command is used, the switch returns to the no-password state.

Follow these guidelines when enabling VTP pruning:

- If you enable pruning on the VTP server, it is enabled for the entire management domain.
- Only VLANs included in the pruning-eligible list can be pruned.
- Pruning is supported with VTP version 1 and version 2.

Follow these guidelines when enabling VTP version 2 (v2-mode):

- Toggling the version (v2-mode) state modifies certain parameters of certain default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use VTP version 2, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 (**no vtp v2-mode**).
- If all switches in a domain are VTP version 2-capable, you need only to enable VTP 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 or configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, VTP version 2 (**v2-mode**) must be enabled.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use VTP version 1.

Examples

This example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

This example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

This example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

This example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

This example shows how to enable v2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

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

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
switchport trunk pruning	Configures the VLAN pruning-eligible list for ports in trunking mode.
vtp (global configuration)	Configures the VTP filename, interface, domain-name, and mode.

wrr-queue bandwidth

Use the **wrr-queue bandwidth** interface configuration command to assign weighted round robin (WRR) weights to the egress queues on Gigabit-capable ports and 10/100 Ethernet ports. The ratio of the weights is the ratio of frequency in which the WRR scheduler dequeues packets from each queue. Use the **no** form of this command to return to the default setting.

wrr-queue bandwidth *weight1 weight2 weight3 weight4*

no wrr-queue bandwidth

Syntax Description

weight1 weight2 weight3 weight4	The ratio of *weight1*, *weight2*, *weight3*, and *weight4* determines the ratio of the frequency in which the WRR scheduler dequeues packets. Separate each value with a space. The range is 1 to 65536.

Defaults

Weight1, weight2, weight3, and weight4 are 25 (1/4 of the bandwidth is allocated to each queue).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(13)EA1	The range changed from 0 to 65536 to 1 to 65536.

Usage Guidelines

The absolute value of each weight is meaningless, and only the ratio of parameters is used.

WRR allows bandwidth sharing at the egress port.

All four queues participate in the WRR unless the expedite queue (queue 4) is enabled, in which case *weight4* 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. You enable the expedite queue by using the **priority-queue out** interface configuration command.

A weight of 1 means that the minimum bandwidth is allocated for that queue.

To allocate no bandwidth for a queue, use the **wrr-queue cos-map** interface configuration command. The available bandwidth is shared among the remaining queues.

Examples

This example shows how to configure the weight ratio of the WRR scheduler running on the egress queues. In this example, four queues are used (no expedite queue), and the ratio of the bandwidth allocated for each queue is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 1/10, 1/5, 3/10, and 2/5 for queues 1, 2, 3, and 4.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue bandwidth 1 2 3 4
```

This example shows how to configure the weight ratio of WRR if the expedite queue is enabled. Three queues participate in WRR, and the bandwidth allocated for each queue is 1/(1+2+3), 2/(1+2+3), 3/(1+2+3), which is 1/6, 1/3, and 1/2 for queues 1, 2, and 3. The last parameter, 9, is not used to calculate the bandwidth ratio.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# priority-queue out
Switch(config-if)# wrr-queue bandwidth 1 2 3 9
```

You can verify your settings by entering the **show mls qos interface queueing** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays quality of service (QoS) information.
wrr-queue cos-map	Maps assigned class of service (CoS) values to select one of the egress queues.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.

wrr-queue cos-map

Use the **wrr-queue cos-map** interface configuration command to map assigned class of service (CoS) values to select one of the egress queues. Use the form **no** of this command to return the CoS map to the default setting.

wrr-queue cos-map *queue-id cos1 ... cos8*

no wrr-queue cos-map [*queue-id* [*cos1 ... cos8*]]

Syntax Description

queue-id	ID of the egress queue. The range is 1 to 4, where 4 can be configured as the expedite queue.
cos1 ... cos8	CoS values that are mapped to select a queue. Enter up to eight CoS values. Separate each value with a space. The range is 0 to 7.

Defaults

Table 2-35 shows the default CoS-to-egress-queue map when QoS is enabled.

Table 2-35 Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	Queue Selected
0, 1	1
2, 3	2
4, 5	3
6, 7	4

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(12c)EA1	CoS values were added to the **no** form of this command.

Usage Guidelines

When quality of service (QoS) is disabled, all CoS values are mapped to queue 1.

You can use this command to distribute traffic into different queues, where each queue is configured with different weighted round robin (WRR) and Weighted Random Early Detection (WRED) parameters.

You enable the expedite queue by using the **priority-queue out** interface configuration command.

Examples

This example shows how to map CoS values 0 and 1 to queue 1, 2 and 3 to queue 2, 4 and 5 to queue 3, 6 and 7 to queue 4:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue cos-map 1 0 1
Switch(config-if)# wrr-queue cos-map 2 2 3
Switch(config-if)# wrr-queue cos-map 3 4 5
Switch(config-if)# wrr-queue cos-map 4 6 7
```

You can verify your settings by entering the **show mls qos interface queueing** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface queueing	Displays the queueing strategy (WRR, priority queueing), the weights corresponding to the queues, and the CoS-to-egress-queue map.
wrr-queue dscp-map	Maps DSCP values to the tail-drop or WRED thresholds of the egress queues.

wrr-queue dscp-map

Use the **wrr-queue dscp-map** interface configuration command on an ingress Gigabit-capable Ethernet port to map the Differentiated Services Code Point (DSCP) values to the tail-drop or Weighted Random Early Detection (WRED) thresholds of the egress queues. Use the form **no** of this command to return the DSCP map to the default setting.

wrr-queue dscp-map *threshold-id dscp1 ... dscp8*

no wrr-queue dscp-map [*threshold-id*]

Syntax Description

threshold-id	Threshold ID of the queue. The range is 1 to 2.
dscp1 ... dscp8	DSCP values that are mapped to a threshold ID. Enter up to eight DSCP values per command. Separate each value with a space. The range is 0 to 63.

Defaults

All DSCP values are mapped to threshold 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Up to eight DSCP values can be entered per command.

Examples

This example shows how to map DSCP values 0 to 9 to threshold 1 and 10 to 14 to threshold 2:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue dscp-map 1 0 1 2 3 4 5 6 7
Switch(config-if)# wrr-queue dscp-map 1 8 9
Switch(config-if)# wrr-queue dscp-map 2 10 11 12 13 14
```

You can verify your settings by entering the **show running-config** or the **show mls qos interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays quality of service (QoS) information.
wrr-queue cos-map	Maps assigned class of service (CoS) ingress values to select one of the egress queues.
wrr-queue random-detect max-threshold	Enables WRED and assigns two WRED threshold values to an egress queue of a Gigabit-capable Ethernet port.
wrr-queue threshold	Assigns tail-drop threshold percentages to an egress queue of a Gigabit-capable Ethernet port.

wrr-queue min-reserve

Use the **wrr-queue min-reserve** interface configuration command to assign a minimum-reserve level to a particular egress queue of a 10/100 Ethernet port. Use the **no** form of this command to return to the default setting.

wrr-queue min-reserve *queue-id min-reserve-level*

no wrr-queue min-reserve *queue-id*

Syntax Description

queue-id	ID of the egress queue. The range is 1 to 4.
min-reserve-level	One of the eight minimum-reserve levels configured with the **mls qos min-reserve** global configuration command.

Defaults

Queue 1 selects minimum-reserve level 1, queue 2 selects minimum-reserve level 2, queue 3 selects minimum-reserve level 3, and queue 4 selects minimum-reserve level 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

You can assign the same minimum-reserve level to multiple queues. Each queue is allocated the same amount of buffer space.

When you enter this command, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets to this queue.

Examples

This example shows how to configure minimum-reserve level 5 to 20 packets and assign minimum-reserve level 5 to egress queue 1 on a port:

```
Switch(config)# mls qos min-reserve 5 20
Switch(config)# interface fastethernet0/1
Switch(config-if)# wrr-queue min-reserve 1 5
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
mls qos min-reserve	Configures the minimum-reserve levels on 10/100 Ethernet ports.
show mls qos interface	Displays quality of service (QoS) information.

wrr-queue queue-limit

Use the **wrr-queue queue-limit** interface configuration command to configure the sizes of the egress queues on Gigabit-capable Ethernet ports. Use the **no** form of this command to return to the default setting.

wrr-queue queue-limit *weight1 weight2 weight3 weight4*

no wrr-queue queue-limit

Syntax Description

weight1 weight2 weight3 weight4	Ratio of *weight1*, *weight2*, *weight3*, and *weight4* determines the ratio of the sizes of the queues. Separate each value with a space. The weight range is 1 to 100.

Defaults

Weight1, weight2, weight3, and weight4 are 25 (1/4 of the buffer size is allocated to each queue).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The relative size differences in the numbers show the relative differences in the queue sizes.

On Gigabit-capable Ethernet ports, the total size of the queue can vary depending on the amount of RAM in the switch.

When you enter this command, the queue is temporarily shut down during the hardware reconfiguration, and the switch drops newly arrived packets to this queue.

Examples

This example shows how to configure the buffer size ratio of the four queues. The ratio of the buffer allocated for each queue is 1/10, 1/5, 3/10 and 2/5 to queue 1, 2, 3, and 4. (Queue 4 is four times larger than queue 1, twice as large as queue 2, and 1.33 times as large as queue 3.)

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue queue-limit 1 2 3 4
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays QoS information.
wrr-queue bandwidth	Assigns weighted round robin (WRR) weights to the egress queues.
wrr-queue min-reserve	Configures the sizes of the minimum-reserve threshold values of the queues on 10/100 Ethernet ports.

wrr-queue random-detect max-threshold

Use the **wrr-queue random-detect max-threshold** interface configuration command to enable Weighted Random Early Detection (WRED) and assign two WRED threshold values to an egress queue of a Gigabit-capable Ethernet port. Use the **no** form of this command to return to the default setting.

wrr-queue random-detect max-threshold *queue-id threshold-percentage1 threshold-percentage2*

no wrr-queue random-detect max-threshold *queue-id*

Syntax Description

queue-id	ID of the queue. The range is 1 to 4, where 4 can be configured as the expedite queue.
threshold-percentage1 *threshold-percentage2*	Maximum threshold percentage values configured per queue. Each threshold percentage represents (average queue size divided by queue size) where WRED starts dropping packets. The WRED minimum threshold value is always 0 when the average queue size equals the allocated queue size. Separate each value with a space. The percentage range is 1 to 100.

Defaults

WRED is disabled, and no thresholds are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Quality of service (QoS) uses the DSCP-to-threshold map to determine which Differentiated Services Code Points (DSCPs) are mapped to threshold 1 and threshold 2. After a threshold is exceeded, WRED randomly begins to drop packets assigned to this threshold. As the queue limit is approached, WRED continues to drop more and more packets. When the queue limit is reached, WRED drops all packets assigned to the threshold.

You can enable WRED on the egress expedite queue by using the **priority-queue out** interface configuration command.

You configure the DSCP-to-threshold map by using the **wrr-queue dscp-map** interface configuration command on the ingress interface.

The **wrr-queue random-detect max-threshold** and the **wrr-queue threshold** commands are mutually exclusive, and only WRED or tail-drop thresholds can be configured.

When you enter the **no wrr-queue random-detect max-threshold** *queue-id* command, tail drop is enabled with the maximum threshold values set to 100 percent.

Examples

This example shows how to configure the WRED maximum threshold values for queue 1 from 50 to 100 percent, for queue 2 from 70 to 100 percent, for queue 3 from 50 to 100 percent, and for queue 4 from 70 to 100 percent:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue random-detect max-threshold 1 50 100
Switch(config-if)# wrr-queue random-detect max-threshold 2 70 100
Switch(config-if)# wrr-queue random-detect max-threshold 3 50 100
Switch(config-if)# wrr-queue random-detect max-threshold 4 70 100
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays QoS information.
wrr-queue dscp-map	Maps DSCP values to the tail-drop or WRED thresholds of the egress queues.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.

wrr-queue threshold

Use the **wrr-queue threshold** interface configuration command to assign tail-drop threshold percentages to each egress queue of a Gigabit-capable Ethernet port. Use the **no** form of this command to return to the default setting.

wrr-queue threshold *queue-id threshold-percentage1 threshold-percentage2*

no wrr-queue threshold *queue-id*

Syntax Description

queue-id	ID of the egress queue. The range is 1 to 4, where the higher ID has a higher priority.
threshold-percentage1 threshold-percentage2	Two tail-drop 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 percentage range is 1 to 100.

Defaults

When QoS is enabled, tail-drop is enabled.

The tail-drop thresholds are 100 percent for both thresholds 1 and 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

QoS uses the DSCP-to-threshold map to determine which Differentiated Services Code Points (DSCPs) are mapped to threshold 1 and threshold 2. If threshold 1 is exceeded, packets with 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.

You configure the DSCP-to-threshold map by using the **wrr-queue dscp-map** interface configuration command on the ingress interface.

The **wrr-queue threshold** and the **wrr-queue random-detect threshold** commands are mutually exclusive, and only tail-drop or Weighted Random Early Detection (WRED) thresholds can be configured.

Examples

This example shows how to configure the tail-drop thresholds of the four queues. The queue 1 thresholds are 50% and 100%; the queue 2 thresholds are 70% and 100%; queue 3 are thresholds are 80% and 100%; queue 4 thresholds are 100% and 100%.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# wrr-queue threshold 1 50 100
Switch(config-if)# wrr-queue threshold 2 70 100
Switch(config-if)# wrr-queue threshold 3 80 100
Switch(config-if)# wrr-queue threshold 4 100 100
```

You can verify your settings by entering the **show mls qos interface buffers** privileged EXEC command.

Related Commands

Command	Description
show mls qos interface	Displays QoS information.
wrr-queue dscp-map	Maps DSCP values to the tail-drop or WRED thresholds of the egress queues.
wrr-queue queue-limit	Configures the sizes of the egress queues on Gigabit-capable Ethernet ports.

Catalyst 3550 Switch Boot Loader Commands

During normal boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot, 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 boot loader 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 boot process while the switch is powering up and then entering a new password. The password recovery disable feature for Catalyst 3550 Fast Ethernet switches allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the boot 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 boot loader 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 boot loader *Switch:* prompt. The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

boot

Use the **boot** boot loader command to load and boot an executable image, and enter the command-line interface.

boot [**-post**] *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.
*filesystem***:**	Alias for a flash file system. Use **flash:** 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 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

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot 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 the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Examples

This example shows how to boot 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.

Related Commands

Command	Description
set	Sets the BOOT environment variable to boot a specific image when the **BOOT** keyword is appended to the command.

cat

Use the **cat** boot loader command to display the contents of one or more files.

cat *filesystem*:*/file-url* ...

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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:

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: ipservices-122-25.SEB
version_directory: c3550-ipservices-mz.122-25.SEB
image_name: c3550-ipservices-mz.122-25.SEB.bin
ios_image_file_size: 6074880
total_image_file_size: 7736832
image_feature: IP|LAYER_3|PLUS|SSH|3DES|MIN_DRAM_MEG=64
image_family: C3550
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands

Command	Description
more	Displays the contents of one or more files.
type	Displays the contents of one or more files.

copy

Use the **copy** boot loader 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 *block-size*	(Optional) This option is used only for internal development and testing.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*source-file-url*	Path (directory) and filename (source) to be copied.
/*destination-file-url*	Path (directory) and filename of the destination.

Defaults

The default block size is 4 KB.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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***:** boot loader command.

Related Commands

Command	Description
delete	Deletes one or more files from the specified file system.

delete

Use the **delete** boot loader command to delete one or more files from the specified file system.

delete *filesystem***:**/*file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	Path (directory) and filename to delete. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The switch prompts you for confirmation before deleting each file.

Examples

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:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

dir

Use the **dir** boot loader command to display a list of files and directories on the specified file system.

dir *filesystem***:**/*file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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 1993 00:48:15  config.text
   11  -rwx        1140   Mar 01 1993 04:18:48  vlan.dat
   21  -rwx          26   Mar 01 1993 00:01:39  env_vars
    9  drwx         768   Mar 01 1993 23:11:42  html
   16  -rwx        1037   Mar 01 1993 00:01:11  config.text
   14  -rwx        1099   Mar 01 1993 01:14:05  homepage.htm
   22  -rwx          96   Mar 01 1993 00:01:39  system_env_vars
   17  drwx         192   Mar 06 1993 23:22:03  c3550-ipservices-mz.122-25.SEB

15998976 bytes total (6397440 bytes free)
```

Table A-1 describes the fields in the display.

Table A-1 dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories.
rmdir	Removes one or more directories.

flash_init

Use the **flash_init** boot loader 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

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

During the normal boot 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** boot loader command to format the specified file system and destroy all data in that file system.

format *filesystem***:**

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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** boot loader command to check the file system for consistency.

fsck [**-test** | **-f**] *filesystem***:**

Syntax Description

-test	(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.
-f	(Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.

Defaults

No file system check is performed.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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** boot loader command to display the available commands.

help

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

You can also use the question mark (?) to display a list of available boot loader commands.

load_helper

Use the **load_helper** boot loader command to load and initialize one or more helper images, which extend or patch the functionality of the boot loader.

load_helper *filesystem***:**/*file-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and a list of loadable helper files to dynamically load during loader initialization. Separate each image name with a semicolon.

Defaults

No helper files are loaded.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **load_helper** command searches for loadable files only if the HELPER environment variable is set.

Filenames and directory names are case sensitive.

memory

Use the **memory** boot loader command to display memory heap utilization information.

memory

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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)
Stack:  0x00746f94 - 0x00756f94 (0x00010000 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 A-2 describes the fields in the display.

Table A-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.
Stack	Beginning and ending address of the area in memory allocated to the software to store automatic variables, return addresses, and so forth.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.

mkdir

Use the **mkdir** boot loader command to create one or more new directories on the specified file system.

mkdir *filesystem***:**/*directory-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*directory-url*	Name of the directories to create. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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***:** boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
rmdir	Removes one or more directories from the specified file system.

more

Use the **more** boot loader command to display the contents of one or more files.

more *filesystem*:*/file-url* ...

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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:

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: ipservices-122-25.SEB
version_directory: c3550-ipservices-mz.122-25.SEB
mage_name: c3550-ipservices-mz.122-25.SEB.bin
ios_image_file_size: 6074880
total_image_file_size: 7736832
image_feature: IP|LAYER_3|PLUS|SSH|3DES|MIN_DRAM_MEG=64
image_family: C3550
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.
type	Displays the contents of one or more files.

rename

Use the **rename** boot loader command to rename a file.

rename *filesystem***:**/*source-file-url filesystem***:**/*destination-file-url*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*source-file-url*	Original path (directory) and filename.
/*destination-file-url*	New path (directory) and filename.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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***:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

reset

Use the **reset** boot loader 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

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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
boot	Loads and boots an executable image and enters the command-line interface.

rmdir

Use the **rmdir** boot loader command to remove one or more empty directories from the specified file system.

rmdir *filesystem***:**/*directory-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*directory-url*	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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.

Examples

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***:** boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
mkdir	Creates one or more new directories on the specified file system.

set

Use the **set** boot loader command to set or display environment variables, which can be used to control the boot loader or any other software running on the switch.

set *variable value*

Note Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

variable value	Use one of these keywords for *variable* and *value*: **MANUAL_BOOT**—Decides whether the switch automatically or manually boots. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode. **BOOT** *filesystem***:/***file-url*—A semicolon-separated list of executable files to try to load and execute when automatically booting. 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 the first bootable file that it can find in the flash file system. **ENABLE_BREAK**—Decides whether the automatic boot 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 boot process by pressing the Break key on the console after the flash file system has initialized. **HELPER** *filesystem***:/***file-url*—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader. **PS1** *prompt*—A string that is used as the command-line prompt in boot loader mode. **CONFIG_FILE flash:/***file-url*—The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. **CONFIG_BUFSIZE** *size*—The buffer size that Cisco IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation. The range is 4096 to 524288 bytes. **BAUD** *rate*—The rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is 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.

BOOTHLPR *filesystem:/file-url*—The name of the Cisco IOS helper image that is first loaded into memory so that it can then load a second Cisco IOS image into memory and launch it. This variable is used only for internal development and testing.

HELPER_CONFIG_FILE *filesystem:/file-url*—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 boot 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

CONFIG_BUFSIZE: 32 KB

BAUD: 9600 bps

BOOTHLPR: No default value (no helper images are specified).

HELPER_CONFIG_FILE: No default value (no helper configuration file is specified).

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

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables are stored in files as shown in Table A-3.

Table A-3 Environment Variables Storage Location

Environment Variable	Location (file system:filename)
BAUD, ENABLE_BREAK, CONFIG_BUFSIZE, CONFIG_FILE, MANUAL_BOOT, PS1	flash:env_vars
BOOT, BOOTHLPR, HELPER, HELPER_CONFIG_FILE	flash:system_env_vars

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 CONFIG_BUFSIZE environment variable can also be set by using the **boot buffersize** *size* global configuration command.

The BOOTHLPR environment variable can also be set by using the **boot boothlpr** *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 boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

Examples

This example shows how to change the boot loader prompt:

```
switch: set PS1 loader:
loader:
```

You can verify your setting by using the **set** boot loader command.

Related Commands

Command	Description
unset	Resets one or more environment variables to its previous setting.

type

Use the **type** boot loader command to display the contents of one or more files.

type *filesystem***:***/file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

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:

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: ipservices-122-25.SEB
version_directory: c3550-ipservices-mz.122-25.SEB
mage_name: c3550-ipservices-mz.122-25.SEB.bin
ios_image_file_size: 6074880
total_image_file_size: 7736832
image_feature: IP|LAYER_3|PLUS|SSH|3DES|MIN_DRAM_MEG=64
image_family: C3550
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.
more	Displays the contents of one or more files.

unset

Use the **unset** boot loader command to reset one or more environment variables.

unset *variable* ...

Note Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

variable	Use one of these keywords for *variable*:
	MANUAL_BOOT—Decides whether the switch automatically or manually boots.
	BOOT—Resets the list of executable files to try to load and execute when automatically booting. 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 the first bootable file that it can find in the flash file system.
	ENABLE_BREAK—Decides whether the automatic boot process can be interrupted by using the Break key on the console after the flash file system has been initialized.
	HELPER—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1—A string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	CONFIG_BUFSIZE—Resets the buffer size that Cisco IOS uses to hold a copy of the configuration file in memory.
	BAUD—Resets the rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.
	BOOTHLPR—Resets the name of the Cisco IOS helper image that is first loaded into memory so that it can then load a second Cisco IOS image into memory and launch it. This variable is used only for internal development and testing.
	HELPER_CONFIG_FILE—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 Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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 CONFIG_FILE_BUFSIZE environment variable can also be reset by using the **no boot buffersize** global configuration command.

The BOOTHLPR environment variable can also be reset by using the **no boot boothlpr** global configuration command.

The HELPER_CONFIG_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

Examples

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

Related Commands

Command	Description
set	Sets or displays environment variables.

version

Use the **version** boot loader command to display the boot loader version.

version

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Examples

This example shows how to display the boot loader version:

```
switch: version
C3550 Boot Loader (C3550-HBOOT-M) Version 12.1(4)EA1
Compiled Wed 21-Feb-01 14:58 by devgoyal
switch:
```

Catalyst 3550 Switch Debug Commands

This appendix describes only the Catalyst 3550-specific **debug** privileged EXEC commands. 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 acltcam

Use the **debug acltcam** privileged EXEC command to enable debugging of the actions of the quality of service/access control list (QoS/ACL) ternary content addressable memory (TCAM) manager software module. This module controls the allocation and updating of entries in the parts of the TCAM used for input security ACLs, output security ACLs, and QoS ACLs. Use the **no** form of this command to disable debugging.

debug acltcam [**verbose**]

no debug acltcam [**verbose**]

Syntax Description

verbose	(Optional) Display detailed debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug acltcam** command is the same as the **no debug acltcam** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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 arguments or keywords.

Defaults

Auto-QoS debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.
12.1(20)EA2	The command changed from **debug autoqos** to **debug auto qos**.

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 fastethernet0/1
Switch(config-if)# auto qos voip trust
Switch(config-if)#
4d22h:mls qos map cos-dscp 0 8 16 26 32 46 48 56
4d22h:mls qos min-reserve 5 170
4d22h:mls qos min-reserve 6 85
4d22h:mls qos min-reserve 7 51
4d22h:mls qos min-reserve 8 34
4d22h:mls qos
4d22h:interface FastEthernet0/1
4d22h: mls qos trust cos
4d22h: wrr-queue bandwidth 10 20 70 1
4d22h: wrr-queue min-reserve 1 5
4d22h: wrr-queue min-reserve 2 6
4d22h: wrr-queue min-reserve 3 7
```

```
4d22h: wrr-queue min-reserve 4 8
4d22h: no wrr-queue cos-map
4d22h: wrr-queue cos-map 1 0 1
4d22h: wrr-queue cos-map 2 2 4
4d22h: wrr-queue cos-map 3 3 6 7
4d22h: wrr-queue cos-map 4 5
4d22h: priority-queue out
```

Related Commands

Command	Description
auto qos voip	Configure auto-QoS for voice over IP (VoIP) within a QoS domain.
show auto qos	Displays the configuration applied and the new defaults in effect when auto-QoS is enabled.
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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**}

no debug backup {**all** | **errors** | **events**}

Syntax Description

all	Display all backup interface debug messages.
errors	Display backup interface error or exception debug messages.
events	Display backup interface event debug messages.

Command Default

Backup interface debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

Usage Guidelines

The **undebug backup** command is the same as the **no debug backup** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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** | **snmp** | **vqpxy**}

no debug cluster {**discovery** | **events** | **extended** | **hsrp** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **snmp** | **vqpxy**}

Syntax Description

discovery	Display cluster discovery debug messages.
events	Display cluster event debug messages.
extended	Display extended discovery debug messages.
hsrp	Display the Hot Standby Router Protocol (HSRP) debug messages.
http	Display HTTP debug messages.
ip [**packet**]	Display IP or transport packet debug messages.
members	Display cluster member debug messages.
nat	Display Network Address Translation (NAT) debug messages.
neighbors	Display cluster neighbor debug messages.
snmp	Display Simple Network Management Protocol (SNMP) debug messages.
vqpxy	Display VLAN Query Protocol (VQP) proxy debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug cluster** command is the same as the **no debug cluster** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show cluster	Displays the cluster status and a summary of the cluster to which the switch belongs.
show cluster candidates	Displays a list of candidate switches when entered on the command switch.
show cluster members	Displays information about cluster members when executed on the command switch.

debug cpu-interface

Use the **debug cpu-interface** privileged EXEC command to enable debugging of the driver for the application-specific integrated circuit (ASIC) that interfaces the CPU to the switch ASIC. Use the **no** form of this command to disable debugging.

debug cpu-interface

no debug cpu-interface

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug cpu-interface** command is the same as the **no debug cpu-interface** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.**ystem Management Commands** > **Troubleshooting Commands**.

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

all	Display all IEEE 802.1x authentication debug messages.
errors	Display IEEE 802.1x error debug messages.
events	Display IEEE 802.1x event debug messages.
feature	Display IEEE 802.1x feature debug messages.
packets	Display IEEE 802.1x packet debug messages.
registry	Display IEEE 802.1x registry invocation debug messages.
state-machine	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
12.1(8)EA1	This command was introduced.
12.1(14)EA1	The **authsm**, **backend**, **besm**, **core**, and **reauthsm** keywords were removed. The **errors**, **events**, **packets registry**, and **state-machine** keywords were added.
12.2(25)SEE	The **feature** keyword was added.

Usage Guidelines

The **undebug dot1x** command is the same as the **no debug dot1x** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show dot1x	Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the 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

all	Display all EAP debug messages.
authenticator	Display authenticator debug messages.
errors	Display EAP error debug messages.
events	Display EAP event debug messages.
md5	Display EAP-MD5 debug messages.
packets	Display EAP packet debug messages.
peer	Display EAP peer debug messages.
sm	Display EAP state-machine related-events debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.

Usage Guidelines

The **undebug dot1x** command is the same as the **no debug dot1x** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, see the **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show eap	Displays EAP registration and session information for the switch or for the specified port.

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 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

all	(Optional) Display all EtherChannel debug messages.
detail	(Optional) Display detailed EtherChannel debug messages.
error	(Optional) Display EtherChannel error debug messages.
event	(Optional) Display major EtherChannel event debug messages.
idb	(Optional) Display Port Aggregation Protocol (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

Release	Modification
12.1(4)EA1	This command was introduced.

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
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show etherchannel	Displays EtherChannel information for the channel.

debug ethernet-controller ram-access

Use the **debug ethernet-controller ram-access** privileged EXEC command to enable debugging of the driver that controls reads from and writes to the private (not directly accessible by the CPU) RAM connected to the forwarding application-specific integrated circuits (ASICs). Use the **no** form of this command to disable debugging.

debug ethernet-controller ram-access

no debug ethernet-controller ram-access

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug ethernet-controller ram-access** command is the same as the **no debug ethernet-controller ram-access** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug fallback-bridging

Use the **debug fallback-bridging** privileged EXEC command to enable debugging of the fallback bridging manager software module. This command debugs the platform-specific part of the process of learning MAC addresses on bridge groups and updating the hardware with the necessary information. Use the **no** form of this command to disable debugging.

debug fallback-bridging

no debug fallback-bridging

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug fallback-bridging** command is the same as the **no debug fallback-bridging** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug gigastack

Use the **debug gigastack** privileged EXEC command to enable debugging of the driver actions for the GigaStack Gigabit Interface Converter (GBIC). Use the **no** form of this command to disable debugging.

debug gigastack

no debug gigastack

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug gigastack** command is the same as the **no debug gigastack** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug ilpower controller

Use the **debug ilpower controller** privileged EXEC command to enable debugging of the platform-specific Power over Ethernet (PoE) software module on the Catalyst 3550-24PWR switch in long message format. These messages include the Power Controller register reading. Use the **no** form of this command to disable debugging.

debug ilpower controller

no debug ilpower controller

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

The **undebug ilpower controller** command is the same as the **no debug ilpower controller**.

Related Commands

Command	Description
debug ilpower event	Enables debugging of the platform-specific PoE software module in a short message format.

debug ilpower event

Use the **debug ilpower event** privileged EXEC command to enable debugging of the platform-specific Power over Ethernet (PoE) software module on the Catalyst 3550-24PWR switch in a short message format. These messages display the PoE state and events received. Use the **no** form of this command to disable debugging.

debug ilpower event

no debug ilpower event

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EA1	This command was introduced.

Usage Guidelines

The **undebug ilpower event** command is the same as the **no debug ilpower event**.

Related Commands

Command	Description
debug ilpower controller	Enables debugging of the platform-specific PoE software module in long message format.

debug ip dhcp snooping

Use the **debug ip dhcp snooping** privileged EXEC command to enable debugging of DHCP snooping events. Use the **no** form of this command to disable debugging.

debug ip dhcp snooping {**acl** | **event** | **packet**}

no debug ip dhcp snooping {**acl** | **event** | **packet**}

Syntax Description

acl	Display all DHCP-snooping access control list (ACL) debug messages.
event	Display all DHCP snooping event debug messages.
packet	Display all DHCP snooping packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(19)EA1	This command was introduced.

Usage Guidelines

The **undebug ip dhcp snooping** command is the same as the **no ip debug dhcp snooping** command.

Related Commands

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

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

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

The **undebug ip igmp filter** command is the same as the **no debug ip igmp filter** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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 group 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

Release	Modification
12.1(8)EA1	This command was introduced.

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
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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

Release	Modification
12.2(25)SEA	This command was introduced.

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
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug l3multicast

Use the **debug l3multicast** privileged EXEC command to enable debugging of the platform-specific Layer 3 IP multicast manager software module, which maintains platform-specific data describing IP multicast routes. Use the **no** form of this command to disable debugging.

debug l3multicast

no debug l3multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug l3multicast** command is the same as the **no debug l3multicast** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug l3tcam

Use the **debug l3tcam** privileged EXEC command to enable debugging of the Layer 3 ternary content addressable memory (TCAM) manager software module. This module controls the allocation of the part of the TCAM used in IP unicast and multicast routing, including the allocation of both routes and adjacencies in the TCAM. Use the **no** form of this command to disable debugging.

debug l3tcam

no debug l3tcam

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug l3tcam** command is the same as the **no debug l3tcam** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug l3unicast

Use the **debug l3unicast** privileged EXEC command to enable debugging of the Layer 3 IP unicast manager. It maintains platform-specific data describing the IP forwarding information base (FIB) entries (routes and adjacencies) and ARP table entries. Use the **no** form of this command to disable debugging.

debug l3unicast

no debug l3unicast

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug l3unicast** command is the same as the **no debug l3unicast** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

debug mac-manager

Use the **debug mac-manager** privileged EXEC command to enable debugging of the platform-specific MAC address table manager software module. This command debugs the platform-specific part of learning MAC addresses on VLANs and updating the hardware with the necessary information. Use the **no** form of this command to disable debugging.

debug mac-manager

no debug mac-manager

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug mac-manager** command is the same as the **no debug mac-manager** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

The **undebug mac-notification** command is the same as the **no debug mac-notification** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show mac address-table notification	Displays the MAC address notification information for all interfaces or the specified interface.

debug met

Use the **debug met** privileged EXEC command to enable debugging of the allocation, freeing, and updating of the multicast expansion table (MET) entries. These entries are used by the hardware when forwarding individual IP multicast and fallback-bridged packets to multiple output VLANs. Use the **no** form of this command to disable debugging.

debug met

no debug met

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug met** command is the same as the **no debug met** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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

all	Display all MVR activity debug messages.
events	Display MVR event-handling debug messages.
igmpsn	Display MVR Internet Group Management Protocol (IGMP) snooping-activity debug messages.
management	Display MVR management-activity debug messages.
ports	Display MVR port debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug mvrdbg** command is the same as the **no debug mvrdbg** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show mvr	Displays the current MVR configuration.

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** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Display all PAgP debug messages.
event	(Optional) Display PAgP event debug messages.
fsm	(Optional) Display PAgP finite state-machine debug messages.
misc	(Optional) Display miscellaneous PAgP debug messages.
packet	(Optional) Display PAgP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug pagp** command is the same as **no debug pagp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show pagp	Displays PAgP channel-group information.

debug pbr

Use the **debug pbr** privileged EXEC command to enable debugging of policy-based routing (PBR) events. Use the **no** form of this command to disable debugging.

debug pbr [**acl-merge**]

no debug pbr [**acl-merge**]

Syntax Description

acl-merge	(Optional) Display debug messages for the merge of ACLs present in a route-map that are applied to an interface for PBR.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(13)EA1	This command was introduced.

Usage Guidelines

The **undebug pbr** command is the same as the **no debug pbr** command.

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

all	Display all dynamic ARP inspection debug messages.
error	Display dynamic ARP inspection error debug messages.
event	Display dynamic ARP inspection event debug messages.
packet	Display dynamic ARP inspection packet-related debug messages.
rpc	Display dynamic ARP inspection remote procedure call (RPC) request debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

The **undebug platform ip arp inspection** command is the same as the **no debug platform ip arp inspection** command.

Related Commands

Command	Description
show ip arp inspection	Displays the dynamic ARP inspection configuration and operating state.
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **sm** | **span** | **split** | **vlan** | **vp**}

no debug pm {**all** | **assert** | **card** | **cookies** | **etherchnl** | **messages** | **port** | **registry** | **sm** | **span** | **split** | **vlan** | **vp**}

Syntax Description

all	Display all PM debug messages.
assert	Display assert debug messages.
card	Display line-card related-event debug messages.
cookies	Display internal PM cookie validation debug messages.
etherchnl	Display EtherChannel related-event debug messages.
messages	Display PM messages debug messages.
port	Display port-related event debug messages.
registry	Display PM registry invocation debug messages.
sm	Display state-machine related-event debug messages.
span	Display spanning-tree related-event debug messages.
split	Display split-processor debug messages.
vlan	Display VLAN related-event debug messages.
vp	Display virtual port related-event 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

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug pm** command is the same as the **no debug pm** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.

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

Release	Modification
12.1(8)EA1	This command was introduced.

Usage Guidelines

The **undebug port-security** command is the same as the **no debug port-security** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show port-security	Displays port-security settings for an interface or for the switch.

debug span-session

Use the **debug span-session** privileged EXEC command to enable debugging of events occurring in the platform-specific software that implements the Switched Port Analyzer (SPAN) feature. Use the **no** form of this command to disable debugging.

debug span-session

no debug span-session

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA1	This command was introduced.

Usage Guidelines

The **undebug span-session** command is the same as the **no debug span-session** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show monitor	Displays SPAN session information.

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** | **csuf/csrt** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

no debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **csuf/csrt** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **uplinkfast**}

Syntax Description

all	Display all spanning-tree debug messages.
backbonefast	Display Backbonefast-event debug messages.
bpdu	Display spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Display optimized BPDU handling debug messages.
config	Display spanning-tree configuration change debug messages.
csuf/csrt	Display cross-stack UplinkFast activity debug messages.
etherchannel	Display EtherChannel-support debug messages.
events	Display spanning-tree topology event debug messages.
exceptions	Display spanning-tree exception debug messages.
general	Display general spanning-tree activity debug messages.
mstp	Display Multiple Spanning Tree Protocol event debug messages.
pvst+	Display per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Display spanning-tree root-event debug messages.
snmp	Display spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	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.
synchronization	Display the spanning-tree synchronization event debug messages.
uplinkfast	Display UplinkFast-event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **mstp** and **csuf/csrt** keywords were added.

Usage Guidelines

The **undebug spanning-tree** command is the same as the **no debug spanning-tree** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	Displays spanning-tree state information.

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**]

Syntax Description

detail	(Optional) Display detailed BackboneFast debug messages.
exceptions	(Optional) Display spanning-tree BackboneFast-exception debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug spanning-tree backbonefast** command is the same as the **no debug spanning-tree backbonefast** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** privileged EXEC command to enable debugging of received and transmitted 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**]

Syntax Description

receive	(Optional) Display receive BPDU debug messages.
transmit	(Optional) Display transmit BPDU debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	Displays spanning-tree state information.

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 unit (BPDU) 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**]

Syntax Description

detail	(Optional) Display detailed optimized BPDU-handling debug messages.
packet	(Optional) Display packet-level optimized BPDU-handling debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug spanning-tree bpdu-opt** command is the same as the **no debug spanning-tree bpdu-opt** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	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

all	Display all the debug messages.
boundary	Display flag changes at these boundaries: • An MST region and a single spanning-tree region running RSTP • An MST region and a single spanning-tree region running IEEE 802.1D • An MST region and another MST region with a different configuration
bpdu-rx	Display the received MST bridge protocol data unit (BPDU) debug messages.
bpdu-tx	Display transmitted MST BPDU debug messages.
errors	Display MSTP error debug messages.
flush	Display the port flushing mechanism debug messages.
init	Display the initialization of the MSTP data structure debug messages.
migration	Display the protocol migration state-machine debug messages.
pm	Display MSTP port-manager event debug messages.
proposals	Display debug messages for handshake messages between the designated and root switch.
region	Display debug messages for the region synchronization between the switch processor (SP) and the route processor (RP).
roles	Display MSTP role debug messages.
sanity_check	Display the received BPDU sanity check debug messages.
sync	Display the port synchronization event debug messages.
tc	Display topology change notification event debug messages.
timers	Display debug messages for the MSTP timers for start, stop, and expire events.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EA1	This command was introduced.

Usage Guidelines

The **undebug spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	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** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

no debug spanning-tree switch {**all** | **errors** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

Syntax Description

all	Display all spanning-tree switch debug messages.
errors	Display debug messages for the interface between the spanning-tree software module and the port manager software module.
general	Display general event debug messages.
helper	Display spanning-tree helper task debug messages. Helper tasks handle bulk spanning-tree updates.
pm	Display port manager event debug messages.
rx	Display received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: **decode**—Display decoded received packets. **errors**—Display receive error debug messages. **interrupt**—Display interrupt service request (ISRs) debug messages. **process**—Display process receive BPDU debug messages. **state**—Display spanning-tree port state change debug messages.
tx [**decode**]	Display transmitted BPDU handling debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **helper** keyword was added.

Usage Guidelines

The **undebug spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	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**]

Syntax Description

exceptions	(Optional) Display spanning-tree UplinkFast-exception debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug spanning-tree uplinkfast** command is the same as the **no debug spanning-tree uplinkfast** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show spanning-tree	Displays spanning-tree state information.

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** | **notification** | **packets** | **registries** | **vtp**}

no debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**}| **events** | **ifs** | **management** | **notification** | **packets** | **registries** | **vtp**}

Syntax Description

badpmcookies	Display debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan {**bootup** | **cli**}	Display config-vlan debug messages. The keywords have these meanings: • **bootup—**Display messages when the switch is booting up. • **cli—**Display messages generated when the command-line interface (CLI) is in config-vlan mode.
events	Display VLAN manager event debug messages.
ifs	Display VLAN manager Cisco IOS file system (IFS) error test debug messages.
management	Display VLAN manager management of internal VLAN debug messages.
notification	Display VLAN manager notification debug messages.
packets	Display packet handling and encapsulation process debug messages.
registries	Display VLAN manager registry debug messages.
vtp	Display the VLAN Trunking Protocol (VTP) debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.1(9)EA1	The **cfg-vlan** keyword was added.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.
show vtp	Displays general information about VTP management domain, status, and counters.

debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable VLAN manager Cisco 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**}

Syntax Description

open {**read** | **write**	Display VLAN manager IFS file-open operation debug messages. The keywords have these meanings: • **read**—Display VLAN manager IFS file-read operation debug messages. • **write**—Display VLAN manager IFS file-write operation debug messages.
read {**1** | **2** | **3** | **4**}	Display file-read operation debug messages for the specified error test (1, 2, 3, or 4).
write	Display file-write operation debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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.

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show vlan	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 messages that trace 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

accfwdchange	Display debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Display debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Display debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Display debug messages for VLAN manager notification of interface link-state changes.
modechange	Display debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Display debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Display debug messages for VLAN manager notification of interface state changes.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show vlan	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

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**] | **xmit**}

no debug sw-vlan vtp {**events** | **packets** | **pruning** [**packets** | **xmit**] | **xmit**}

Syntax Description

events	Display debug messages for general-purpose logic flow and detailed VTP debugging messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Display debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning [**packets** | **xmit**]	Display debug messages generated by the pruning segment of the VTP code. The keywords have these meanings: • **packets—**(Optional) Display debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer. • **xmit—**(Optional) Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
xmit	Display debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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.

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show vtp	Displays general information about VTP management domain, status, and counters.

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 debugging.

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

Syntax Description

events	Display debugging messages for UDLD process events as they occur.
packets	Display debugging 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.
registries	Display debugging messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)EA1	This command was introduced.

Usage Guidelines

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:

- Subblock creation
- Fiber-optic port status changes
- State change indications from the port manager software
- MAC address registry calls

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References** > **Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2** > **System Management** > **Troubleshooting and Fault Management**.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

P

Q

R

S

T

U

V

W